International Journal of Grid and Distributed Computing
Vol. 9, No. 1 (2016), pp.201-206
http://dx.doi.org/10.14257/ijgdc.2016.9.1.20

SURVEY: Reputation and Trust Management in VANETs

Jitendra Singh Sengar

BVM College of Technology & Management,
Gwalior, MP, India

jitendrasinghsengar@gmail.com

Abstract

This paper concerns reputation and trust computation in vehicular ad hoc networks (VANETs). Various survey and implemented work has been studied and analyzed to form a new survey on trust model to VANET. In this survey 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. Trust management in VANET (TMV) is one well know concept and basic need to maintain a reliable secure faith full VANET on which node may believe through their close eye and could drive for safe journey with ultimate faith.

Keywords: *V2V, V2I, VANET, TMV*

Introduction

In a VANET node communicate each other by sharing information of road condition like traffic jam accidental alert and form safety on the basis of theses thing while driving, some more effort has been putted to develop life critical & road condition related system like traffic visibility system, message sharing, collision detection & avoidance and crash reporting all these activity must be in safe manner. 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 message to mislead and to spreads spam messages to create problem like false information of traffic jam accident and robbery. Various trust models reviewed some of them are deployed. With difference in their architecture, their trust establishment processes is shown in below section trusted system creation. In this paper Some important section elaborated to build effective trust model which would provide best security with safety from spam spread by unauthorized node in VANET**.** The important point out the security objective, security requirement, safety in VANET and trust establishment model which is described to understand the entire security system of VANET.

Reputation and trust are two essentials tools of security that are used to facilitate decision making in VANETs. In general, reputation is the opinion of one entity as vehicles in VANETs about another [3]. Essentially it signifies the trustworthiness of a vehicle in VANETs. Trust in general is the level of confidence in a person or a thing [4]. In VANETs, it is the expectation of one vehicle about the action of another vehicle [5].

TRUST-

TRUST MANAGEMENT-

Philosophical view Management of trust are 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 lot of faith to break, corrupt and destroy the entire system of VANET. Various issues occur to create faith full environment in VANET. Some of them are described below.

TRUST MANAGEMENT ISSUES-

SECURITY OBJECTIVES

It is impossible that node take responsibility to provide their location detail and impersonation. Another requirement is that data and control packets must be free from loops and directed only to their actual target destination. Due to volatile nature of network it is not required to forward packets on short route paths towards target destination.

SECURITY REQUIREMENT

Above security objectives could be related to the traditional security requirement. There are essential and significant in order to maintain a reliable and secure Ad-hoc VANET environment.

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

Availability: Data must be available any time. Network service unavailability would be possible by 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 entire network area make confidentially.

Integrity: the originality of data from adversary and /or harsh environment ensured to avoid inconsistence.

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

SAFETY IN VANET

Safety-related applications play their role in VANET and underlie special requirements [14] and constraints; car driving on a highway could detect emergency braking because of an accident and communicates this event to other cars on the same highway. Cars driving behind the sender receive this message have to decide whether to display warning messages to their drivers or not. To take this decision the cars need to evaluate the trustworthiness.

TRUST ESTABLISHMENT

There are two basic options for trust establishment:

1. SELF ORGANIZING TRUST ESTABLISHMENT-

- Direct: Direct Trust is established on the behalf of mutual communication with other nodes.
- Indirect: Nodes exchange information about other nodes and their trust relationships. This implies that trust relationships are transitive.
- Hybrid: combines both direct and indirect mechanisms in the following, several approaches for self organizing trust establishment will be discussed.

2. ESTABLISHMENT BASED ON INFRASTRUCTURE

2.1 BLIND SIGNATURE:

Chaum introduce first Blind signature scheme. property of RSA used in it. It based on elliptic curve cryptography can be used interchangeably; this scheme can be used to certify pseudonyms with basic cause of some security issues, such as: There is no way to ensure non-repudiation and certificate revocation, since newly signed pseudonyms cannot be linked to authenticator/node

2.1.1 The signed pseudonyms may be used to launch Sybil attacks, and we cannot deal with it since there is no way to link pseudonyms with each other or with the true identity of the node.

A node with valid authenticator may share its pseudonyms with another node that does not have a valid authenticator and who is unable to get pseudonyms.

A: 1. Generate random number r: gcd $(r, n)=1$
2. Compute blinding factor bf: $bf = re$
3. Blind message m to m' : $m' = bf\ m = (re\ m)$ mod n
A _ B: 4. m'
B: 5. Sign message m' using private key d: $x = (m')d$ mod n
B _ A: 6. X
A: 7. Recover message signature: $s = md = r\text{-}1(x)$mod n 8. $r\text{-}1(x)$mod $n = r\text{-}1(m')d$ mod $n = r\text{-}1(re\ m)d$ mod $n = r\text{-}1r\ md$ mod $n = md$ mod n Figure 1. Basic Blind signature scheme (public key parameters: n, e = public
key of B and d= secret key of B).

- ZERO KNOWLEDGE/NIZKP:

These approaches can also be used for the establishment of anonymity; one node proves to another node the trust of an assertion (its certified statement) with knowledge of secret information (its ID) without revealing it. The main concept of NIZK proofs is the prover’s and verifier’s access to a common random string (public randomness). That is also the reason why NIZK[11] proofs are a very promising concept for trust establishment in VANETs. The only problem we found is its still questionable applicability.

- GROUP SIGNATURE:

Group of person issue a private key that could be used to generate signatures which verify public key. Outside member can only verify that a signature which generated by some member of the group but cannot get member information. This approach maintained by central authority, which resolve signatures to each nodes, which had been issued the according to the private key made by group member.

EXISTING RELATED WORK

In related work a proposed AHP based technique has seen in which there are three steps. These three steps constitute trust value of vehicle using AHP [17] method.

1. Reputation based trust computation: the trust value in these steps depends upon vehicles previous records. When vehicle is not listed in revocation then trust value is 1 otherwise 0. Reputation based trust value is denoted by Reputation of vehicle ie rep_trust value parameter. If some vehicles are police cars and traffic controllers,School vans, Post office vans the reputation will also 1.

2. *Direct Rank Computation:* The direct ranking trust computation is also based on message strength. This method is computed by Perron–Frobenius theorem based on message strength, each participant vehicle can compute trust value based on the messages received from other vehicles. The computed trust value depends on both the outcome of the message veracity and strength of messages. If message is communicated just after authenticated by any mechanism in VANET, the value of should be more, after that it should be decreased after a period of time. Another method is to distribute the one value per transaction between vehicles in a continuous, rather than discrete way. One way to assign a value to is to distribute the point on the basis of the message strength. If vehicle receives points (weighted sum of correct messages) and points (weighted sum of incorrect messages, (weights being different for correct and incorrect message of same priority)) during a communication session.
3. *Rank Computation:* In the last step, the indirect rank computation is based on evaluation the number of authentication certificate exchange at the certain time of vehicles within communication range proposed AHP based trust computation technique for VANET has been evaluated through simulation of real traffic scenarios. A road with multiple unidirectional lanes is considered. Packet length is considered 153 bytes for vehicle to vehicle communication.

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. The indirect rank is denoted by In the AHP based trust value of the vehicle is from the above illustration, it can be observed that the AHP based trust computation can be used to associate trust values with vehicles.

The mechanism is able to consider different types of information for computation of the trust values. The authors discuss some key design constraints of the solution which are given below:

□It provides the anonymity of inter-vehicular communication particularly and avoids the use of

Same cryptographic pseudonym for long period of time. An authorized administrator provides the entity of possibility to revoke the anonymity of a given message. □It uses native TPM security mechanism□ it has the possibility to downgrade the standard operation if an entity does not operate correctly.

CONCLUSION & Future Strategy

The conclusion of entire study is that here lot of way to pointing the research interest, here free file of same domain has been defined and briefly described. Our proposed work would be in this area to perform effective job in trust modeling, issues and security attack in VANET. This paper help to increase researchers to put their effort in new direction of 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 new precaution from the attract & new approach for security & safety is politically proposed by our future coming proposed paper.

References

[1] L. A. Martucci, M. Kohlweiss, C. Anderson, A. Panchenko, "Self-certified Sybil-free pseudonyms", Proceedings of the First ACM Conference on Wireless Network Security, New York, NY, USA, ACM Press, **(2008)**, pp. 154–159.

[2] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks". Journal of Computer Security, vol. 15, no. 1, **(2007)**, pp. 39–68.

[3] K. Govindan, P. Mohapatra, "*Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey"* IEEE Communications Surveys Tutorials, vol. PP, no.99, **(2011)**, pp. 1-20.

[4] A. Tajeddine, A. Kayssi, A. Chehab, "*A Privacy-Preserving Trust Model for VANETs,*" International Conference on Computer and Information Technology, China 2011

[5] Huibin Xu and DaiWei Wen, "A trust-based routing protocol in ANET," In IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 2, pp. 260-263, 2013.

[6] B. K. Chaurasia and R. S. Tomar, "Trust Management Model for Wireless Ad hoc Networks", Proceedings of the International Conf. on SocProS2011, AISC 130, vol. 1, **(2012)**, pp. 193-198.

[7] B.K. Chaurasia, S. Verma, G.S. Tomar, "Intersection Attack on Anonymity in VANET", Springer Trans. on Comput. Sci. Vol.17, LNCS 7420, pp. 133–149, 2013.

[8] M. Rahbari and M. Ali Jabreil Jamali, "EfficientDetection od Sybil Attack Based on Cryptography in Vanet" International Journal of Network Security & Its pplications (IJNSA), vol.3, no.6, **(2011)**.

[9] S. Goudarzi1, A. H. Abdullah2, S. Mandala2, S. A. Soleymani2 "A Systematic Review of Security in Vehicular Ad Hoc Network".

[10] TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks

[11] M.-C. Chuang and J.-F. Lee, "One-way-linkable Blind Signature Security Architecture for VANET", Baber Aslam and Cliff C. Zou Dept. of Electrical Engineering and Computer Science University of Central Florida, Orlando, FL, USA

[12] AHP Based Trust Model in VANETs, 2013 5th International Conference on Computational Intelligence and Communication Networks

[13] B.K. Chaurasia, S. Verma & G. S. Tomar, "Mechanism for Privacy Preservation in VANETS", International Journal of Grid and High Performance Computing, vol.2, no.2, **(2010)**, pp. 12-22.