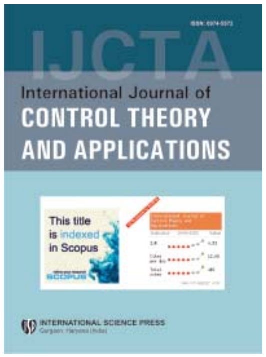

International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 9 • Number 40 • 2016

Identification of Location Falsifying Vehicle in A Vehicular Cloud

S. Hemavathy[a] and K. Venkatesh[b]

[a]Dept. of Information Technology, SRM University, Kattankulathur-603203, Chennai, India.
E-mail: hemavathysathyasugu@gmail.com
[b]Assistant Professor, Dept. of Information Technology SRM University, Kattankulathur-603203, Chennai, India.
E-mail: venkatesh.k@ktr.srmuniv.ac.in

Abstract: Trust management traffic control system helps to pass emergency vehicles effortlessly. Secure interoperable wireless communications network which includes traffic signals, buses, cars, mobile phones and other devices have the ability to transform the way natives travel through VANETs (Vehicular ad hoc networks). However, VANETs are accountable to security threats because of rising dependence on compute, communication and control technologies. The distinctive security and privacy problems posed by VANETs include secrecy, reliability, access control, non-repudiation, privacy protection and availability. The reliability of VANETs could be enhanced by reported traffic data are trustworthy and node trust. In this research, an ART (Attack-resistant trust) Scheme that evaluates the reliability of both data and mobile nodes in VANETs, are able to cope and detect malicious attacks. Node trust is assessed in two proportions, that is recommendation and functional trust, which point out how trustworthy the recommendations is, between nodes and how likely a node can fulfill its function; Data trust is assessed based on the data collected and sensed from various vehicles respectively. The thought behind the system is to execute an effortless control of traffic and helps emergency vehicles to arrive at the destination. Improved mobility, environmental protection and traffic safety with improved Trustworthiness are made as a trigger to cloud service so that it can be viewed by the users in the VANET.

Keywords: *Vehicular ad hoc networks (VANETs); emergency vehicle; trust management; security; trustworthiness.*

1. INTRODUCTION

The difficulty of traffic management arises especially for emergency vehicles. The initiative of easy management of traffic helps the emergency vehicle to reach the target. The growing needs for improved road safety and effectiveness of transportation system have stimulated vehicle producers to fit in wireless communications and networking into vehicles. The wirelessly networked vehicles naturally form Vehicular Ad-hoc Networks (VANETs), in which vehicles unite to spread various data messages, without the need of central supervision. In VANETs, various nodes, such as Roadside Units (RSUs) and vehicles are generally equipped with processing, sensing and wireless communication capabilities.

The safety applications which provide warnings regarding traffic conditions (I., emergency braking, congestion), road accidents, and other pertinent transportation incidents are through V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) which helps for communications. Although, VANETs are susceptible towards threats, owing to cumulative reliance on technologies, control communication and computing. The distinctive safety and confidentiality challenges posed by VANETs include access control [1], data trust (integrity), real-time operational constraints/demands [2], no repudiation [3], privacy protection [4] and availability [5]. The traveler information and the analytical evidence needed for active traffic is been managed by a typical application of VANETs known as Traffic Estimation and Prediction System (TrEPS) [6]. TrEPS will simplify and enhance real-time advanced transportation systems operation, operational evaluation and planning analysis. All these evolving information need networking support, such as VANETs, to resourcefully share and distribute the collected traffic information. If the trustworthiness of the sensor data cannot be properly evaluated, then it is possible to produce traffic jams or even life-threatening road accidents because most of the vehicles will be incorrectly redirected to the same route if the fake traffic alerts remain undetected and thus effective in VANETs, which may causes serious threat to the life of native in the emergency vehicle. Therefore, it is important to secure VANETs so that they can better support smart transportation applications such as TrEPS for the navigation of emergency vehicle.

When related with the traditional wired networks, VANETs themselves are more vulnerable to malicious attacks because of their specific features, like highly dynamic network topology, limited supply of power and error-free transmission media. For instance, the wireless communication links among vehicles are disposed to both passive eavesdropping and active tampering. Thus, it is critical to detect and cope with malicious attacks in VANETs so that the security of natives, drivers and vehicles in addition to the effectiveness of the transportation system can be better guaranteed. The trustworthiness of VANETs could be enhanced by tackling both data trust and node trust. In this research, an Attack-Resistant Trust scheme (ART) is put forward to cope with malicious attack and also to evaluate data integrity as well as nodes in VANETs. In the ART scheme, the trustworthiness of data and node as two separate metrics, namely data trust and node trust, respectively. In specific, data trust is used to evaluate whether or not and to what level the traffic data detail is trustworthy. On the other hand, node trust indicates how reliable the nodes in VANETs are. It could guarantee a comprehensible path for an emergency vehicle to guard someone’s life. Malicious nodes in VANETs can be detected using ART scheme.

1. Firstly, an attack-resistant trust management scheme is studied in this paper, which can detect effectively and cope with multiple types of malicious behaviors in VANETs.

2. Second, the data identified and collected from numerous vehicles assess the trustworthiness of traffic data (data trust).

3. Third, the trustworthiness of vehicle nodes is made as a vector that is composed of two elements, that is functional and recommendation trust which indicates how one node can justify its function and also how trustworthy the recommendations between nodes.

4. Fourth, the proposed ART scheme can effectively assess the trustworthiness of both sensed mobile nodes and data in VANETs to guarantee a comprehensive path for the emergency vehicle.

   Finally, the trustworthiness of the node are been triggered to the cloud service, so that the user can easily identify the trustworthiness of the vehicles node in the vehicular cloud.

2. RELATED WORK

2.1. Trust Management in Ad hoc Networks

The key reason for the trust management is for evaluating the multiple performances of the other nodes also to establish a reputation for every distinct node depending on the behavior assessment of every node. The reputation for every distinct node can be developed to determine the trustworthiness, create opportunities to liaise for which node it has to take and also necessary action is taken to rebuke an un-trusted node from the network if needed to be. Generally, node behaviors is been evaluated based on two types of interpretations by using trust management. Direct observation which is known as first hand observations [7]. First hand observation is directly made by the node itself, and could be collected likewise actively or passively. If the nodes only make a constant monitor of its neighbors' activities, the observation of information which is local is been collected passively. On the other hand, the reputation management system could depend on few explicit proofs to calculate the behavior of neighbor, such as acknowledgement packet in the process of route discovery. Another observation of information is known as indirect observation otherwise known as second hand observation. Second hand observation which is commonly determined by interchanging the first hand observation of information by the other nodes in the network. One major disadvantage of the second hand observation is associated with the collision, false report and also overhead of information in the nodes.

Buchegger came up with a protocol named CONFIDENT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks) [8], in order to inspire the nodes cooperation and also remove the misbehaving nodes in the network. CONFIDANT is made up of four different components in each node: a Reputation system, a monitor, a Path to identify and observe Manager, made use of irregular routing behaviors. Then the Reputation Management System evaluates every individual nodes reputation in agreement with the behaviors which is been observed. The message is been interchanged with other alternate misbehaving nodes by means of the Trust manager. The path is been ranked and maintained by the Path manager and response is been sent regularly to multiple routing messages in the node. One feasible disadvantage in CONFIDENT is that, incorrect messages might spread to other nodes by the attacker purposely, which states that a particular node which is really a well behaved node is marked as misbehaving node in the network. So, it is compulsory for a node in CONFIDENT to authorize the message which is been received before the message is been accepted. Michiardi [9] came up with a working called CORE for cooperating with the routing activities and also recognize the selfish nodes. Similar to the CONFIDENT, CORE makes use of both the surveillance and also the reputation system to assess and observe the behavior of the node. However whilst CONFIDENT permits to interchange negative and also positive observations of their respective nodes neighbors. And only the positive observation are been interchanged among the nodes in CORE.

In such a manner, the misbehaving nodes will not be able to spread false information to corner the well behaving nodes, and accordingly dodge the DOS attack towards the well behaved nodes. The reputation of every node is been preserved by the reputation system and are continuously accustomed upon getting novel evidence. In some cases standings are lesser than other nodes as selfish nodes reject to cooperate. To boost the node cooperation of nodes and also punish the selfishness, and if any other node with a very low reputation sends request for routing, it will be snubbed and other bad reputation node will not be able to make use of the network. Patwardhan [10] presented a technique where the reputation of a few node here, known as the Anchor node, are been pre authenticated, such that the data they provide seems to be trustworthy. Information is been validated through straight communication to an anchor node or agreement among peers. Malicious node may be recognized if the data presented is not validated by the algorithm of validation. In addition, there have been some other research efforts that aim to enhance the security, trust and privacy of VANETs [11]–[16].

Most of the existing trust management methods for adhoc networks focus on assessing the trustworthiness of Mobile nodes by collecting numerous evidences and analyzing prior behavioral history of the nodes. However, little consideration has been paid to evaluate the trustworthiness of the data shared among these nodes as well. Given that the data reliability and trustworthiness in transportation systems are extremely important as well, to evaluate the trustworthiness of both data and mobile nodes in this work.

3. PROBLEM DEFINITION

3.1. Network Model

A VANET generally refers to a wireless network of heterogeneous sensors or other computing devices that are deployed in vehicles. This type of network enables continuous monitoring and sharing of road conditions and status of the transportation systems to guarantee a comprehensible path for emergency vehicles. All of the nodes in VANETs are prepared with the same wireless communication interface, such as IEEE 802.11p. The nodes are limited in energy as well as computational and storage capabilities.

3.2. Adversary Model

The connected vehicles, on the other hand, are generally more susceptible to various attacks, and they can be compromised at any time after the VANET is formed. The adversary can be an outsider located in the wireless range of the vehicles, or the adversary can first compromise one or more vehicles and behave as an insider later. The adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The main goals of the adversary may include intercepting the normal data transmission, forging or modifying data, framing the benign devices by deliberately submitting fake recommendations, etc. More specifically, the following malicious attacks are considered in this paper.

3.3. Cloud Model

The trustworthiness of the node are been triggered to the cloud service, so that the user can easily identify the trustworthiness of the vehicles node in the cloud with the help of ACT schema in the VANET.

4. THE ATTACK-RESISTANT TRUST (ART) SCHEME FOR VANETS

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

4.1. Preliminaries

The In general, the trustworthiness of a node Nk can be defined in the form of a vector $\theta k = (\theta k\ (1), \theta k(2), \ldots ,\theta k(n))$, in which $\theta k(i)$ stands for the overview of the ART scheme. *i-th* aspect of the dependability for the Nk node. Every dimension of the reliability $\theta k(i)$ correlate with category B$k(i)$ for one or a particular behavior(s) (likewise forwarding of packet or real recommendation sharing), and $\theta k(i)$ could appropriately replicate the probability in the node which will be conducting B$k(i)$ in a routine which is suitable for the nodes. $\theta k(i)$ could be allocated to any real type value between the value range of [0,1], *i.e.*, $\forall i \in \{1, 2, \ldots, n\}$, $\theta k(i) \in [0, 1]$. The node Nk is more likely to conduct B$k(i)$ properly, when the value of $\theta k(i)$ is more. Each and every aspect of $\theta k(i)$, which is trustworthy for the Nk node which is established as a function of misbehaviors M$k(i)$ which is correlated to B$k(i)$ that is noted by the neighbor of the Nk device. Diverse aspects of the trustworthiness might agree to diverse functions, where the choice for diverse function must match the bare features of M$k(i)$, which are the occurrence frequency, outcome from severity and also the occurrence due to the situation. To be particular, the trustworthiness of a device is represented in a vector $\theta k = (\theta k(1), \theta k(2))$, and each element in the vector stands for functional trust and recommendation trust, respectively. In the future, if it is necessary to introduce new element to the trust vector, the new element can be added easily.

4.2. Schene Overview

The ART scheme is composed of two phases, namely data analysis and trust management. In the ART scheme, we first collect traffic data from VANETs for data analysis. Second, we summarize the findings from the data analysis as evidences for trust management schemes to evaluate the trustworthiness. Then these evidences will be used to assess the trustworthiness of data and nodes. The trustworthiness of nodes further consists of functional trust and recommendation trust.

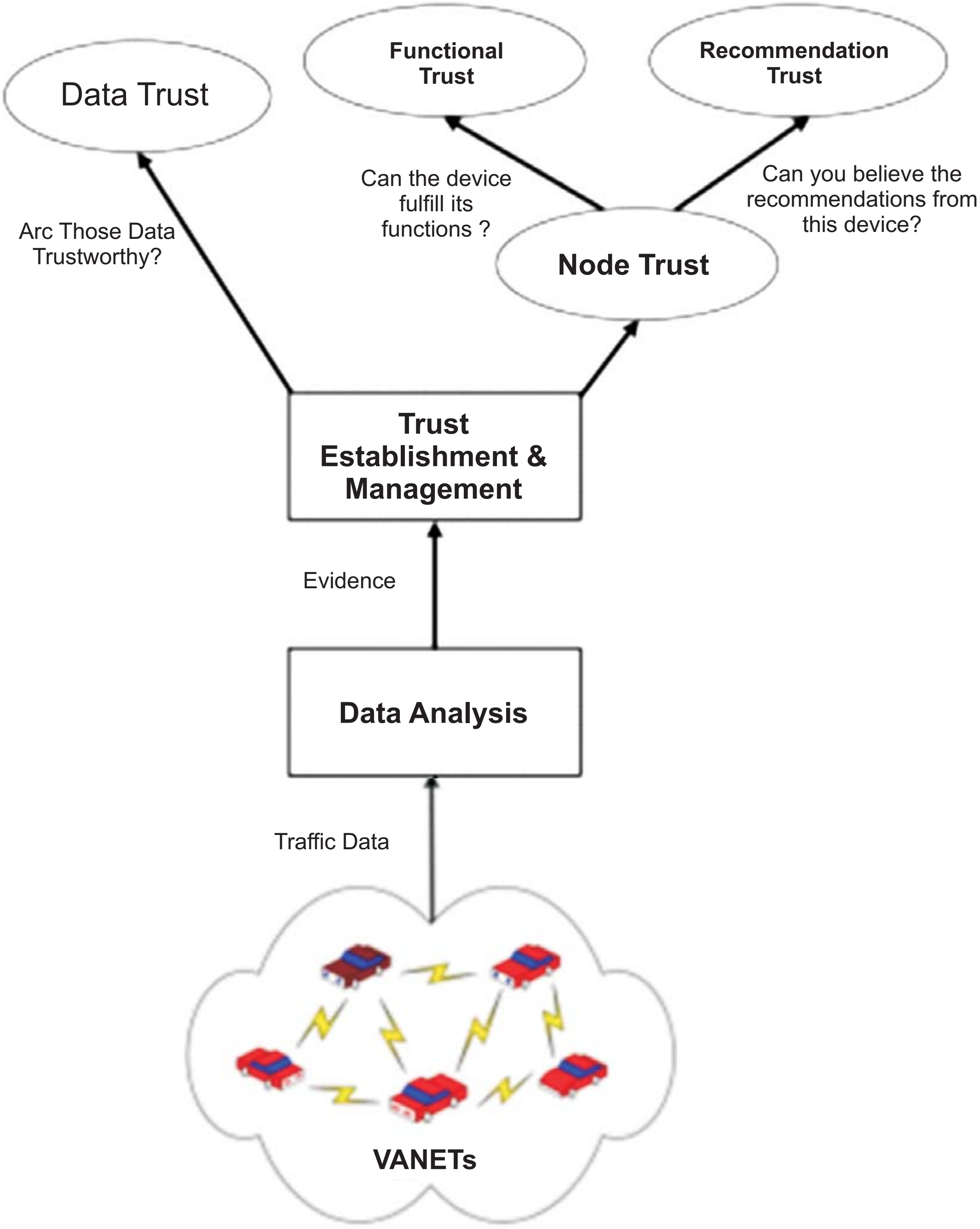
Data Trust
Functional Trust
Recommendation Trust
Can the device fulfill its functions ?
Can you believe the recommendations from this device?
Arc Those Data Trustworthy?
Node Trust
Trust Establishment & Management
Evidence
Data Analysis
Traffic Data
VANETs

Figure 1: Art Scheme

4.3. Evidence Combination

Using the Dempster's rule (DST- Dempster's-Shafer Theory) the modernized evidence for node *i* is been found,

Input of a_i **:** S*i*

Output of a_i **:** S*i*

After receiving S*k* from the node a_i **:**

If S*i* _ = S*k* then

1. **Rendering to the following rules , combine S*i* and S*k* :**

    a) If both S*k* and S*i* are present in node *i*, the updated value of Si is calculated for the equivalent columns where node *i* is in both S*k* and S*i* by using DST combination and S*i* is stocked as an entry in an intermediary list TEMPi.

    b) If either S*k* or S*i* are present in node *i*, a check is made by adding a virtual entry to the node *i* for identifying whether it has any entry *i.e*., 1 and assign all the virtual entry to 0 when there is any entry. The updated value of S*i* is been calculated, from the equivalent columns of node *i* in both S*k* and S*i* by using DST combination and S*i* is stocked as an entry in an intermediary list TEMPi.

2. **Compute the outlier's *k* from TEMPi and these *k* outliers are allocated to S*i*.**

3. **The value of S*i* is broadcasted to all the immediate neighbor nodes (*i.e*., number of hop = 1).**

    Else don't send message out and keep Si unchanged.

    End if

5. CONCLUSION

In this research, an Attack-Resistant Trust (ART) is used for evaluating the trustworthiness of both traffic data and vehicle nodes for VANETs. Due to no delay in the emergency vehicle, there will be no loss of life. It could guarantee a clear path for an emergency vehicle to protect someone's life. In the ART scheme, the trustworthiness of data and nodes are modeled and evaluated as two separate metrics, namely data trust and node trust, respectively. In particular, data trust is used to evaluate whether or not and to what level the traffic data detail is trustworthy. On the other hand, node trust indicates how trustworthy the nodes in VANETs are. ART scheme accurately evaluates the trustworthiness of data as well as nodes in VANETs, and it can also cope with various malicious attacks and trigger the malicious attack information to the cloud service in the cloud.

REFERENCES

[1] R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys" *Comput.Commun.*,vol.44,pp. 1–13,May2014.

[2] M. Kakkasageri and S. Manvi, "Information management in vehicular ad hoc networks: A review" *J. Netw. Comput. Appl.*, vol. 39, pp. 334–350, Mar. 2014.

[3] B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols:Asurvey"*J. Netw. Comput. Appl.*,vol.40,pp.363–396,Apr. 2014.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network" *J. Netw.Comput. Appl.*, vol. 37, pp. 380–392, Jan.2014.

[5] M. Raya and J.-P.Hubaux, "Securing vehicular ad hoc networks" *J. Comput. Security*, vol. 15,no. 1 pp. 39–68, Jan. 2007.

[6] Y. Lin and H. Song, "DynaCHINA: Real-time traffic estimation and prediction," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 65–65, Oct.–Dec. 2006.

[7] S. Buchegger and J.-Y. L. Boudec, “A robust reputation system for mobile ad-hoc networks,” in *Proc. P2PEcon*, Berkeley, CA, USA, 2003,pp. 1–6.

[8] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the confidant protocol,” in *Proc. 3rd ACM Int. Symp. MobiHocNetw.Comput.*,Lausanne, Switzerland, 2002, pp. 226–236.

[9] P. Michiardi and R. Molva, “CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in *Proc.IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Security*, Portoroz, Slovenia, 2002, pp.107–121.

[10] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, “A data intensive reputation management scheme for vehicular ad hoc networks,” in *Proc. 3rdAnnu. Int. Conf. Mobiquitous Syst. Workshops*, Jul. 2006, pp. 1–8.

[11] W. Li, A. Joshi, and T. Finin, “Coping with node misbehaviors in ad hoc networks: A multi- imensional trust management approach,” in *Proc.11th Int. Conf. MDM*, May 2010, pp. 112–121.

[12] S. Taha and X. Shen, “A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs,” *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 4, pp. 1665–1680, Dec. 2013.

[13] Z. Li, C. Liu, and C. Chigan, “On secure VANET-based ad dissemination with pragmatic cost and effect control,” *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 124–135, Mar. 2013.

[14] T. Chim, S. Yiu, L. Hui, and V. Li, “OPQ: OT-based private querying in VANETs,” *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1413–1422, Dec. 2011.

[15] R. Lu, X. Lin, X. Liang, and X. Shen, “A dynamic privacy-preserving key management scheme for location-based services in VANETs,” *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar.2012.

[16] G. Rebolledo-Mendez, A. Reyes, S. Paszkowicz, M. Domingo, and L. Skrypchuk, “Developing a body sensor network to detect emotions during driving,” *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no.4,pp.1850–1854,Aug.2014.