Vehicular Communications 2 (2015) 150–157

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

CAT: Consensus-assisted trust estimation of MDS-equipped collaborators in vehicular ad-hoc network

T. Raghu Vamsi Krishna [a], Rajesh P. Barnwal [b,*], Soumya K. Ghosh [a]

[a] *School of Information Technology, Indian Institute of Technology, Kharagpur, 721302, India*
[b] *Information Technology Group, CSIR-Central Mechanical Engineering Research Institute, Durgapur, 713209, India*

ARTICLE INFO

Article history:
Received 6 December 2014
Received in revised form 10 May 2015
Accepted 3 June 2015
Available online 9 June 2015

Keywords:
VANET
Security
Trust
Misbehavior

ABSTRACT

The trust establishment in highly mobile ad-hoc network is a challenging task. Vehicular ad-hoc network (VANET) poses trust estimation problem in dynamic network environment. Presence of misbehavior detection schemes (MDS), in the vehicular node, safeguards them up to a certain extent from misbehaving vehicles but existing MDS algorithms have their own limitations in terms of capability and accuracy. In this scenario, vehicles are supposed to collaborate among themselves for getting better assessment of the misbehaving peers. However, the trustworthiness of collaborators is always a questionable factor subject to verification. Trust estimation of the collaborating nodes is essentially required to provide supplementary information for more accurate decision about the adversaries. In this paper, algorithms have been proposed to estimate trustworthiness of the MDS-equipped collaborating nodes with the help of consensus mechanism. After comparison of different proposed trust-estimation algorithms in simulated environment, results reveal that the unsupervised *k*-means based consensus clustering algorithm is an effective solution for precise estimation of the trustworthiness of the collaborating node.

1. Introduction

Majority of the safety applications, developed for Vehicular Ad-hoc Network (VANET), work by exchange of relevant information or data dissemination [1] among the peers in observing vehicle's close proximity. Several cryptographic primitives [2] have been proposed to provide message integrity, entity authentication and non-repudiation. Even though a vehicle possesses valid credentials, the content of message itself can be forged. This could be due to malfunctioning of devices equipped in a vehicle or may be due to adversaries present in the network. One such threat is called Illusion Attack [3], in which false data is generated by attacker by playing prank on sensors of their own car. For example, a vehicle braking hard suddenly raises an *Emergency Electronic Brake Light* (EEBL) alert. Attacker launches a DOS attack by jamming the network and sends a rear-end vehicle to speed up because of which a collision may occur. To detect such types of behavior, several *Misbehavior Detection Schemes* (MDS) have been proposed [4–9]. However, the quality of these MDS can be affected by capability of devices/sensors in the vehicle. The MDS output (hereinafter called as *MDS value*) signifies the measured level of misbehavior demonstrated by a communicating node. The accuracy of the MDS value is subject to quality and accuracy of the implemented MDS algorithm and sensors of the observing vehicle. In this situation, it is desirable that the vehicles should collaborate and exchange their MDS value among themselves to supplement the limitations of the individual MDS capability. However, the trustworthiness of the collaborating vehicles itself is a subject for verification. For instance, a vehicle collaborating with other vehicles might be an adversary and tries to negatively influence the decision of an observing vehicle.

The contributions of this work are as follows:

- Generic trust model: In this work we proposed a generic model for calculating the trust of MDS-equipped collaborating vehicles during collaborations. Algorithms were proposed to estimate better idea on event with the help of trust on collaborating vehicles.
- Trust based on vehicle's opinion: Algorithms have been proposed for estimating misbehavior value and calculating trust. One algorithm calculates trust based on a threshold value and the other algorithm calculates the trust based on deviation from its MDS value and it is shown that the convergence rate of algorithm, which calculates trust based on the deviation from its MDS value, is faster.

* Corresponding author.
E-mail addresses: vamsi.talanki@gmail.com (T. Raghu Vamsi Krishna), barnwal.r@gmail.com (R.P. Barnwal), skg@iitkgp.ernet.in (S.K. Ghosh).

http://dx.doi.org/10.1016/j.vehcom.2015.06.001
2214-2096/© 2015 Elsevier Inc. All rights reserved.

- Trust based on majority opinion: We have proposed algorithms for finding majority value. We explain how unsupervised k-means clustering can be used for finding majority value. This value has been used for estimating misbehavior value and calculating trust of vehicles. With this approach we are able to obtain a better estimate of misbehavior value and convergence is faster as compared to the trust calculation based on vehicle's MDS value.

Proposed algorithms have been analyzed for studying the effects of percentage of attackers, message loss and node density in the network. The convergence rate of the algorithms has been evaluated empirically to evaluate the real-time applicability of the algorithm.

Remaining part of the paper is organized as follows: Section 2 discusses the existing works for the trust establishment in VANET. Section 3 describes the misbehavior based trust estimation model considered for the present work. Section 4 describes the proposed consensus assisted trust estimation algorithms. The algorithms use independent MDS value and take majority opinions into consideration for estimation of trustworthiness of the collaborators. Section 5 presents the experimental results and analysis of the proposed algorithms. Section 6 concludes the paper.

2. Related work

Consensus-assisted trust estimation is an active area of research. The requirement of consensus is well-appreciated for the security of networked entity [10]. The concept of trustworthiness in network takes help of the consensus mechanism and past experience parameter for making informed and more accurate decision to achieve security. Trust-establishment in ephemeral network of VANET is a challenging task. Jie Zhang's [11] survey on trust management in VANET discusses the key issues of various proposed trust models. It identifies a list of properties that should be achieved by a trust model in the vehicular network scenario. D. Huang et al. [12] used a Situation-aware Trust (SAT) architecture, which utilizes social network trust for inter-vehicle trust establishment. The proposed model uses e-mail based Trust or similar kind of identity-based trust system, which may violate the privacy issue. Moreover, this type of model is not able to address the misbehavior due to faulty components of the vehicle. Minhas et al. [10] proposed aggregation-based enhanced trust management scheme. They used aggregation of several different trust metrics to reach to a certain conclusion. The given scheme mainly relies on role-based trust and experience-based trust along with majority opinion. The concept seems to be effective but the main problem in the concept is the method of gathering consensus from peers. Here, the algorithm needs the advice to be sought by the vehicle from its neighbors. In response, the neighbors have to send their opinion. The algorithm assumes the presence of the same vehicle in the vicinity for a good amount of time at a stretch, so that vehicle receives message and responds to them using unicast. However, in very dynamic scenario, it may not be possible to send the unicast message without proper identification of the agent. Moreover, pseudonyms may also create problem in sending the message on unicast basis. Philippe et al. [13] proposed an approach to check the validity of data in VANET using adversial parsimony heuristic. Fabio et al. [14] proposed probabilistic validation of aggregated data for eliminating malicious vehicles (vehicles reporting false position and velocity information) by verifying proof of the aggregated result given by aggregator. Schmidt et al. proposed VEhicle Behavior Analysis Scheme (VEBAS) [15] to calculate trust on position information, reported in beacon messages by vehicles, by analyzing the behavior of vehicles. The trust of vehicles is calculated using behavior analysis modules, which gives positive and negative ratings based on output of sensors.

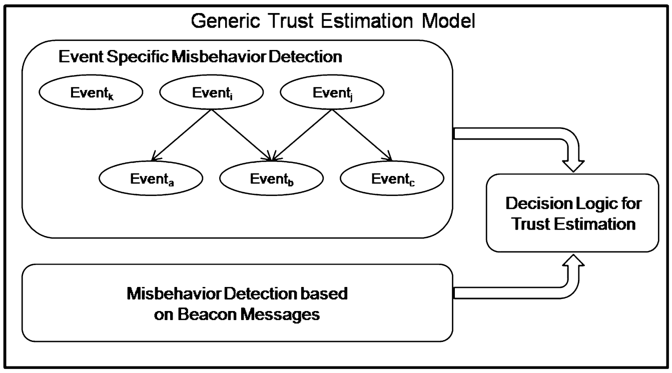
Generic Trust Estimation Model
Event Specific Misbehavior Detection
Event_k
Event_i
Event_j
Event_a
Event_b
Event_c
Decision Logic for Trust Estimation
Misbehavior Detection based on Beacon Messages

Fig. 1. Misbehavior based trust estimation model.

The above shows that the existing trust estimation schemes have their own limitations. Moreover, a number of misbehavior detection schemes [4,5,7,13,16,17] are in place for use in VANET that can be utilized in-turn for trust estimation of a vehicle in VANET. The vehicle may utilize any one or combination of these MDS for misbehavior detection and trust estimation. Thus, there is a need to develop an efficient trust estimation algorithm, which can estimate the trustworthiness of collaborating MDS-equipped vehicle based on independent MDS rating or by considering peers' MDS rating about the event-reporting vehicle.

3. MDS-based trust estimation model

The MDS-based trust estimation model, for trust estimation of reporting nodes, is shown in Fig. 1. In the model, the trust development process is divided into two phases: *Misbehavior detection using independent MDS* and *Trust estimation based on reported MDS value*. Further, a vehicle may use event-specific misbehavior detection scheme [18] or beacon-based misbehavior detection scheme [7] for detection of misbehaving nodes in VANET.

3.1. Event specific misbehavior detection

Whenever an event occurs, the application equipped for perceiving the event notifies about the event. After getting notification about the event, a vehicle calculates the correctness of event reported with the help of respective MDS. It is assumed that each vehicle has its own *Independent MDS* for detection of misbehavior. The misbehavior of a vehicle V, reporting $Event_i$, is also assessed and reported by different collaborating vehicles $(v_1, v_2, \ldots, v_n)$ and is represented by a set $P_i = \{p_1, p_2, p_3, \ldots, p_n\}$ containing misbehavior values $p_1, p_2, p_3, \ldots, p_n$. After getting a set of misbehavior values from collaborating vehicles, the observing vehicle calculates the trust of collaborating vehicles $(v_1, v_2, \ldots, v_n)$.

The alternative method for assessment of the trustworthiness of collaborating vehicles is based on vehicle reporting about correlated events. The main motive behind the misbehavior detection based on the correlated events is that whenever an event happens, some correlated events occur accordingly. For instance, the primary events of *post crash notification* (PCN) are supposed to be followed by different correlated secondary events such as *slow vehicle alerts* (SVA), *emergency electronic brake light* (EEBL), and *lane change alerts* (LCA) [18]. However, this may not be true for all the events. The subset ε^i of ε contains the events that occur as a result of primary $event_i$. The arrows in Fig. 1 show the occurrence of events as result of a primary event. Events a and b occur because of $event_i$, while events b and c occur because of $event_j$. If there is no correlated event for a particular primary event, this module returns a value