Trust Management for VANETs: Challenges, Desired Properties and Future Directions

Jie Zhang, Nanyang Technological University, Singapore

ABSTRACT

An increasingly large number of cars are being equipped with GPS and Wi-Fi devices, forming vehicular ad-hoc networks (VANETs) and enabling vehicle to vehicle communication with the goal of providing increased passenger and road safety. However, dishonest peers (vehicles) in a VANET may send out false information to maximize their own utility. Given the dire consequences of acting on false information in this context, there is a serious need to establish trust among peers. This article first discusses the challenges for trust management caused by the important characteristics of VANET environments, and identifies desired properties that effective trust management should incorporate in order to address the challenges. The author then surveys and evaluates existing trust models in VANETs, and points out that none of the trust models has achieved all the properties. Finally, the author proposes some important future directions for research towards effective trust management for VANETs.

Keywords: Road Safety, Traffic Congestion, Trust Management, Vehicle to Vehicle Communications, Vehicular Ad hoc Network

INTRODUCTION

Various studies have established the fact that the number of lives lost in motor vehicle crashes world-wide every year is by far the highest among all the categories of accidental deaths (Wikipedia, n.d.). With the expected increase in the vehicle and human populations as well as economic activities, roads will likely get busier. Thus, there is an urgent need to enhance road safety and reduce traffic congestion. Recently, with the advancement in technology more and more vehicles are being equipped with GPS and Wi-Fi devices that enable vehicle to vehicle (V2V) communication, forming a vehicular ad-hoc network (VANET). Peer vehicles in VANET can communicate with each other regarding up to date information about road and traffic conditions, so as to avoid car accidents and effectively route traffic through dense urban areas. VANET is thus envisioned to be one of the most important applications of mobile ad-hoc networks in the future.

Network-On-Wheels (NOW) project (http://www.network-on-wheels.de/), GST, Prevent and Car-to-Car Consortium (http://www.car-to-car.org/) among others, represent some of the ongoing efforts in the general domain of vehicular networks. Some car manufacturers have already started to fit devices that will help
achieve the goals mentioned above. For example, GM has rolled out V2V communication in its Cadillac STS Sedans. GM’s proprietary algorithm called “threat assessment algorithm” keeps track of the relative position, speed and course of other cars (also equipped with V2V technology) in a quarter-mile radius and issues a warning to the driver when a crash is imminent. Similar prototypes by other car manufacturers are currently in the testing phase, scheduled to hit the markets over the coming years (Nadeem et al., 2004; Xu et al., 2004; Elbatt et al., 2006; Rahman & Hengartner, 2007). These systems focus mainly on ensuring a reliable delivery of messages among peers. As a result, less focus has been placed on evaluating the quality of information that is sent by peers, in order to cope with reports from malicious peers which may compromise the network. For example, consider a peer that reports the roads on his path as congested with the hope that other peers would avoid using these roads, thus clearing the path. Therefore one important issue among others that may arise in VANETs is the notion of trust among different peers.

The goal of incorporating trust is to allow each peer in a VANET to detect dishonest peers as well as malicious data sent by these dishonest peers, and to give incentives for these peers to behave honestly and discourage self-interested behavior. Given the critical nature of the applications in the context of VANETs, it is crucial to associate trust with peers and the data that they spread. However, due to the important and possibly unique characteristics of VANET environments, effectively modeling trust of peers becomes very challenging.

In this article, which is an extended version of Zhang (2011), we first discuss the challenges for trust management caused by the large, decentralized, open, sparse and highly dynamic nature of VANET environments, and identify some key desired properties that trust management should incorporate, including decentralized trust establishment, being capable of coping with sparsity, being event/task and location/time specific, scalable, robust and sensitive to privacy concerns, and integrated confidence measure. For each property, we also extensively discuss some trust models proposed in other domains (such as multi-agent systems, peer-to-peer systems, collaborative intrusion detection networks, etc.) that may provide useful solutions. We then survey and evaluate the existing trust models in VANETs based on the desired properties. None of them has achieved all the properties. We finally suggest some important future research directions towards effective trust management in VANETs.

CHALLENGES IN VANET ENVIRONMENTS

Modeling trustworthiness of peers in VANETs presents some unique challenges. First of all, the vehicles in a VANET are constantly roaming around and are highly dynamic. On a typical highway the average speed of a vehicle is about 100 km/hour. At high speeds the time to react to an imminent situation is very critical, therefore, it is very important for the peers to be able to verify/trust incoming information in real-time. Second, the number of peers in VANET can become very large. For example, in dense urban areas the average amount of vehicles that pass through the network may be on the order of millions and several thousand vehicles will be expected to be present in the network at any given time. Also this situation is exacerbated during the rush hours when, for example, majority of the people commute to and back from work in a metropolitan area. This may introduce several issues such as network congestion - since vehicles are communicating on a shared channel, and information overload - resulting from vehicles receiving a lot of data from the near-by vehicles in a congested area (Leckie & Kotagiri, 2003).

Another key challenge in modeling trust in VANET is that a VANET is a decentralized, open system i.e., there is no centralized infrastructure and peers may join and leave the network any time respectively. If a peer is interacting with a vehicle now, it is not guaranteed to interact with the same vehicle in the future (Eichler et al.,
Application of HY-2 Satellite SST Data in 4D Variational Assimilation Ocean Forecast Model