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

DOI: 10.4018/jdst.2012010104

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.,

2006). Also, information about road condition is rapidly changing in VANET environments, e.g., a road might be busy 5 minutes ago but now it is free, making it hard to detect if the peer spreading such information is malicious or not. This also brings out an important challenge that the information received from VANETs needs to be evaluated in a particular context. The two key context elements in VANETs are *location* and *time*. Information which is closer in time and location of an event is of more relevance.

DESIRED TRUST MANAGEMENT FOR VANET

Based on the challenges in VANET environments, we identify here a list of desired properties that effective trust management should incorporate for VANETs.

Decentralized Trust Establishment

Trust establishment should be fully decentralized to be applicable to the highly dynamic and distributed environment of VANETs (Dotzer et al., 2005; Mass & Shehory, 2001; Yu & Singh, 2002a). Many trust models (Wu & Sun, 2001; Regan et al., 2006; Tran, 2005; Minhas et al., 2010a, 2010b), make use of only peers' direct interactions to update one peer's belief in the trustworthiness of another. This kind of one-to-one interaction can easily be implemented in a distributed manner. Some trust models (Yu & Singh, 2000, 2002a, 2002b) also allow a peer *A* to model the reputation of another peer *B* by seeking many other peers' opinions about *B* and combining these opinions together. However, peer *A* may not know which other peers have had direct interactions with *B* because there is no a central authority as in the centralized reputation systems (Jøsang & Ismail, 2002) to collect such information. The models of Yu and Singh (2000, 2002a, 2002b) in distributed peer-to-peer environments thus also allow peer *A* to seek advice from other peers called referrals about which peers may have knowledge about peer *B*. Once the peers who have the required information are identified, reputation of peer *B* can be built in a distributed manner.

And, the trust models (Raya et al., 2007; Sabater & Sierra, 2001; Huynh et al., 2006; Minhas et al., 2010a, 2010b) that rely on the real-world role of vehicle drivers should also be done in a totally decentralized manner among the vehicles themselves. For this to work, car manufacturers or transportation authorities may need to be involved to issue certificates at the manufacture or registration time respectively. A public-private key infrastructure for verifying each other's roles can be implemented in a distributed manner. Mass and Shehory (2001) provide a model that on seeing a certificate enables a third party (or peer) to assign specific roles to the peers in the system. Based on their roles the peers are then supposed to carry our certain duties and are expected to abide by certain policies. In this scenario, any peer can act as a certificate issuer and thus role assignment is achieved in a distributed fashion.

Coping with Sparsity

Effective trust establishment should not be contingent upon a minimum threshold for direct interactions. As described in the section on Challenges in VANET Environments, it should not be expected that a peer in VANET would possibly interact with the same peer more than once. However, it is important to clarify here that the trust models should still be able to effectively take into consideration any data available from direct interaction (even though it might happen just once). Thus, in a scenario where the number of peers that are able to spread information has gone down to the extent that the condition of information scarcity or a total lack of information is prevalent, any data might be termed valuable. In the trust calculation, the weight for the data can be raised in this scenario while it may have a lower default value, to cope with the data sparsity problem in VANET.

The role-based trust approaches of Raya et al. (2007), Sabater and Sierra (2001), Huynh et al. (2006), and Minhas et al. (2010b, 2010a) can distinguish trustworthy peers from un-

trustworthy ones to some extent despite the sparsity of the environment, as real-world roles of vehicle drivers and the trust associated with these roles are assumed to be pre-defined in these trust models.

The idea of allowing peers to send testing requests in Staab et al. (2008) and Fung et al. (2011) can also deal with sparsity. The senders of these testing requests basically know the solution to these requests in advance. Imaging a group of vehicle drivers driving in a city from one location to another, they remain in contact range for a certain period of time. These drivers can send testing requests to each other and evaluate their feedback. Trust between them can then be established.

Event/Task and Location/ Time Specific

Since the environment of the peers in VANET is changing constantly and rapidly, a good trust model should introduce certain dynamic trust metrics, capturing this dynamism by allowing a peer to control trust management depending on the situation at hand (Raya et al., 2007; Dotzer et al., 2005). Here, we separately discuss two particularly important dynamic factors in the context of VANETs, event/task and location/ time.

Peers in general can report data regarding different events e.g., car crashes, collision warnings, weather conditions and information regarding constructions etc. Trust management should therefore be event/task specific. For example, some of these tasks may be time sensitive and require quick reaction from the peer that receives them. In this case, this peer can only consult a very limited number of other peers to verify whether the reported information is true. In another case, reporting peers having different roles in VANET may have more or less knowledge in different types of tasks. For example, a police may know more about car crash information while city authorities may know more about road construction information. In addition, a peer should update the reporting peer's trust by taking into account the type of the reported event. For example, life-critical events will certainly have more impact on the reporting peer's trust.

We also note that location and time are another two particularly important dynamic metrics. For example, if the origin of a certain message is closer to the location of where the reported event has taken place, it might be given a higher weight, relying on the underlying assumption that a peer closer to the event is likely to report more realistic data about the event (given that they are not malicious themselves). Similarly, we can apply this concept to time. If the message reporting a certain event is received closer to the time when the reported event has taken place, it might be allowed a higher weight in trust calculation. Another suggestion that naturally follows from time based trust is that, since the relevance of data in VANET is highly dependent on when it was received, it would make sense to assign a decay factor to the message. The message further away from the time of evaluating trust would be assigned a lower weight. In other words, we should decay the impact of the message relative to the time of the trust evaluation. The decay factor is somewhat analogous to the time-to-live (TTL) relay decision used in traditional routing algorithms (Li & Wang, 2007).

The first issue that may arise with calculating time or location specific trust is how to get location and time of the actual event. It can be expected that whenever a report regarding an event is generated to be shared among other peers it will hint to the time at which this event has taken place, giving the required time information. Also it can be assumed that every peer while transmitting the report appends its location with the report. The next issue is to verify whether the time and location information contained within a report is real or spoofed. With this regard, Golle et al. (2004) have proposed a method to accurately estimate the location of nearby peers. Now the next task would be to actually use the location/ time information in trust management. In the calculation of subjective reputation as proposed by Sabater and Sierra (2001) they use a weighted

sum of trust values suggesting that the weights should be adjusted such that higher weights are assigned to the peers closer to the peer who is calculating trust. In a similar fashion, one can extend their model by instead of defining the closeness between peers; she can define the location closeness between the actual event and the peer reporting this event. For the time based trust a similar calculation can be done by modifying the notion of time closeness as that between the time when the event has taken place and that of receiving the report.

Scalable

Scalability is an important aspect in trust management in VANET environments. More specifically, in a dense environment, the number of peers reporting information or passing through the network can be potentially very large. On another hand, for critical situations, a peer has to make decisions very quickly. Having this requirement, each peer should consult or accept information from only a number of other trusted peers, as suggested in Minhas et al. (2010b). This number can be fixed or slightly updated with the changes in, for example, VANET size or the task at hand. However, it is always set to a value small enough to account for scalability.

Establishing trust in VANETs should also be scalable. For example, modeling trust based on experience requires each peer to store the history of past interactions with other peers and to compute their trust based on that information. For the purpose of being scalable, trust models should update peers' trustworthiness by accumulatively aggregating peers' past interactions in a recursive manner, similar to Jøsang and Ismail (2002) and Fung et al. (2011). The computation of the peer trust is thus linear with respect to the number of interactions. And only the most recent trust values are needed to be stored and used for computation. This design can make trust management scalable.

In a global sense, false information from a sender peer should be controlled to a local minimum in the scenario where other peers may relay the sender's message. This is to reduce network traffic and increase network scalability. Trust management can be helpful in this case (Chen et al., 2010b) by having peers to decide about whether to relay the sender's message based on the trust value derived for the message. However, there is tradeoff between the global network scalability and trust establishment among peers. On one hand, it is important to have network scalability where a peer should consult only a minimum necessary number of other peers. On another hand, in order to gain more experience with other peers for more accurate trust modeling, this peer has to try out the information from more peers. Fung et al. (2011) propose to adjust the frequency of consulting one peer based on the uncertainty of the modeled trust value of the peer. This peer will be consulted more often if the trust value is above a certain threshold but the uncertainty is high, to increase the confidence on this potentially trustworthy peer. This naturally leads to another feature desired by trust management in VANETs, an integrated confidence measure.

Integrated Confidence Measure

Incomplete information about the other peers induces much uncertainty in modelled trustworthiness values of these peers. It is thus important to include in trust management a confidence measure to capture the uncertainty. Confidence is the accuracy of modelled trust value and usually lies in the interval [0,1]. The value of confidence would depend on the number of different metrics that were available (and their reliability on a per metric basis in a given context) in the calculation of the associated trust value. In general, higher value of confidence i.e., a value closer to 1 would result from considering more evidence or metrics having high reliability. Confidence can be viewed as a parameter that adds another dimensionality to the output generated by the model allowing the peer applications to have a richer notion of trust and finally decide how to react on the reported event.

A number of researchers have proposed trust and reputation models with the notion of

confidence (Huynh et al., 2006; Teacy et al., 2006; Mui et al., 2002). In particular, Huynh et al., (2006) introduced FIRE, a framework that integrates direct trust and role-based trust, in which the direct trust model of Sabater and Sierra (2001) is proposed as the method for capturing this element of the overall calculation, with some adjustment to consider more carefully the decay of trust values over time. FIRE also calculates a confidence value for each dimension of the integrated trust and reputation model based on the reliability of the evidence for modelling the dimensional trust. The TRAVOS model in Teacy et al. (2006) is a trust and reputation model for agent-based virtual organizations. This approach is based on the beta probability density function. It calculates the confidence of a modelled trust value given an acceptable level of error. If the confidence level of a trust value is below a predetermined minimum level, TRAVOS will seek information about the agent being modelled from other agents. A confidence value is calculated by Mui et al. (2002) using the Chernoff Bound theorem based on the amount of evidence and the acceptable level of error.

Wang and Singh (2007) have further extended the notion of confidence to a certainty measure that takes into account not only the number of interactions but also the conflict among the reports of multiple reporting agents. Certainty decreases when conflict among reports increases. Considering the uncertainty property of trust establishment, Balakrishnan et al. (2008) express the notion of ignorance during the establishment of trust relationships between mobile nodes. Subjective logic based model is employed to denote the trust as a three dimensional metric: belief, disbelief, and uncertainty. The uncertainty represents the ignorance between two nodes. Such representation is useful since an existing peer may not have a record of past evidence towards a newcomer/stranger peer, in which case assigning an arbitrary trust value could bring about problems.

In addition, peers may also not be very confident about their reported event because of the incomplete observation of the event. For example, if the distance from the location where the event happens is far and/or the weather condition of the environment is not ideal, the peer may be uncertain about the report event. It is thus valuable to attach a confidence measure to each reported event, as suggested by Chen et al. (2010b).

System Level Security

Security mechanisms at the system level deal with protocols that, among other things, allow peers to authenticate themselves i.e., prove their identity. This is important because most of the trust building models assume that an agent can be uniquely identified. To this end, certain security requirements identified to be essential for trust in multi-agents systems have been identified in Poslad et al. (2002). These requirements include a) Identity - the ability to determine the identity of an agent b) Access permissions - the ability to determine the access rights that are to be assigned to the agents based on its identity c) Content integrity - the ability to be able to tell if a piece of data has been modified since its dispatch from the source agent d) Content privacy - the ability to ensure that only the agents for whom some information is intended are able to examine it. The basic security requirements described above can be implemented through the public-private key infrastructure (PKI) that makes use of public key encryption and certificates. A trusted certification authority (CA) issues a public key certificate verifying that a certain public key is owned by a particular peer, which can simply be a document containing the peer's name or drive license and his public key. The public key then can be used to encrypt and sign a message that allows only the owner to examine the contents and validate its integrity. More specifically, that document is signed by the CA (with the certificate authority's private key) to become the peer's public key certificate. Everyone can verify the authority's signature by using the authority's public key. Now, when peer *A* sends a message to peer *B*, *A* must sign the message with his private key. *B* then can verify (using *A*'s public key) that the message was truly sent by *A*.

Chen et al. (2010a) propose a trust opinion aggregation scheme in vehicular ad-hoc networks, to support trust models used to evaluate the quality of information shared among peers in the environment. Their scheme extends an existing identity-based aggregate signature algorithm to correctly combine signatures for multiple messages into one aggregate signature and eliminate signature redundancy. As a result, the proposed scheme is secure and archives both space efficiency and time efficiency.

Sensitive to Privacy Concerns

Privacy is an important concern in a VANET environment. In this environment, the revealing of a vehicle owner's identity (e.g., the owner's home address) may allow a possibly malicious party to cause damage to the owner. Trust management that makes use of a public key infrastructure (PKI) allows peers to authenticate each other. When a peer sends a report to another peer, the sender needs to authenticate itself to the receiver. Although these keys do not contain any sensitive identities of the sender, the receiver may be able to track them by logging the messages containing the key of the sender. For example, the receiver can track the likely home address of the sender by finding out the route of the sender if the receiver has sufficient information about different locations that the sender has been to, and therefore other identities. This issue can be addressed by changing keys, as suggested in Raya and Hubaux (2007). Each peer in VANET will store a large set of pre-generated keys and certificates. It will change keys while sending information to others regarding some privacy sensitive locations of the sender (i.e., places nearby home), so that others do not recognize this sender as one of the previous senders that they have interacted with. In this way, others will not be able to discover the sender's privacy sensitive identities, while they will still be able to keep track of experience with this sender regarding some insensitive locations of the sender.

Robustness

Trust management can effectively improve peer collaboration in VANETs to share information and detect malicious peers. However, the trust management itself may become the target of attacks and be compromised. We discuss some common attacks and defense mechanisms against them. For example, newcomer attacks occur when a malicious peer can easily register as a new user (Resnick et al., 2000). Such a malicious peer creates a new ID for the purpose of erasing its bad history with other peers in the network. Trust models can handle this type of attacks by assigning low trust values to newcomers, so that the information provided by these peers is simply not considered by other peers for making decisions about whether to follow the information. Only when their trust exceeds a certain threshold, they can then affect others' decisions.

Betrayal attacks occur when a trusted peer suddenly turns into a malicious one and starts sending false information. A trust management system can be degraded dramatically because of this type of attacks. One can employ a mechanism like (Tran, 2005), which is inspired by the social norm: "It takes a long-time interaction and consistent good behavior to build up a high trust, while only a few bad actions to ruin it." Trust of a peer is thus hard to build but easy to lose. Some models, such as Dellarocas (2000), Zhang and Cohen (2008), and Jøsang and Ismail (2002), employ a forgetting factor to assign less weight to older experiences with a peer, or keep only the recent experience with the peer. When the trustworthy peer acts dishonestly, its trust value will drop down quickly, hence making it difficult for this peer to deceive others or gain back its previous trust within a short time period.

Inconsistency attacks are also called on-off attacks and happen when a malicious peer repeatedly changes its behavior from honest to dishonest in order to degrade the efficiency of the network. This kind of attacks is also similar to betrayal attacks but may be less harmful according to the empirical study by Zhang et al.

(2008). It can also be coped with by setting time windows and employing a forgetting factor to assign less weight to older experiences.

Sybil attack occurs when a malicious peer in the system creates a large amount of pseudonyms (fake identities) (Douceur, 2002). This malicious peer uses fake identities to gain larger influence over the false information on others in the network. One possible defense against sybil attacks can rely on the design of the authentication mechanism to make registering fake identities difficult. In the system, the certificate issuing authority only allows one identity per peer using the unique identity, such as driver license. To make such attacks harder to achieve, trust management can also require peers to first build up their trust before they can affect the decision of others, which is costly to do with many fake identities.

However, more than one peer in VANET may form a coalition with others to achieve a common goal. For instance, one such goal could be to cause mayhem in the network which can be attributed to vandalism or terrorism. Unfortunately, even some of the most prominent models (e.g., Sabater & Sierra, 2001) are vulnerable to strategic lying and collusion. Here we would like to point out that this weakness does not specifically come out in the domain of VANETs, however, its consequences can be more critical and might end up claiming many lives. Collusion attack is still an open problem in the area of trust and reputation systems in every domain. Information about how often some peers have supported each other may reveal colluding relationships among them.

EFFECTIVENESS OF EXISTING TRUST MODELS IN VANETS

Only a few trust models have recently been proposed for enforcing honest information sharing in vehicular networks. In this section, we summarize them and evaluate their effectiveness based on the desired properties identified in the previous section. Note that great efforts have been spent by researchers in security and privacy on trust establishment in VANETs that relies on a security infrastructure and most often makes use of certificates (Wex et al., 2008). We focus on trust models that do not fully rely on the static infrastructure and thus can be more easily deployed. These models can be grouped into three categories, entity-oriented trust models, data-oriented trust models, and combined trust models. Entity-oriented trust models focus on the modeling of the trustworthiness of peers. Data-oriented trust models mainly focus on evaluating the trustworthiness of data. In these models, normally, no trust relationships between peers will be formed. Combined trust models make extensive use of peer trust to evaluate the trustworthiness of data, but also maintain peer trust over time.

Two typical entity-oriented trust models are the sociological trust model proposed by Gerlach (2007) and the multi-faceted trust model proposed by Minhas et al. (2010a, 2010b, 2011). The sociological trust model is proposed based on the principle of trust and confidence tagging. Gerlach has identified various forms of trust including situational trust, dispositional trust, and system trust. The multi-faceted trust model features in the role-based trust and experience-based trust as the evaluation metric for the integrated trustworthiness of vehicular entities. The two models have some components in common, for example, situational trust can be compared with event/task specific trust of the multi-faceted trust model, and similarly dispositional trust can be compared to experience or role-based trust.

In contrast to the traditional view of entity-oriented trust, Raya et al. (2007) propose that data-oriented trust may be more appropriate in the domain of VANETs. Data-centric trust establishment deals with evaluating the trustworthiness of the data reported by other entities rather than trust of the entities themselves. They evaluate various evidences regarding a particular event taking into account different trust metrics applicable in the context of a particular vehicular application. Finally their decision logic outputs the level of trust that can be placed in the evaluated evidences indicating whether

Table 1. Properties of the existing trust models for VANET

Approaches	Raya et al., 2008	Dotzer et al., 2005	Golle et al., 2004	Minhas et al., 2010b	Chen et al., 2010b	Gerlach, 2007	Patwardhan et al., 2006
Decentralized	√	√	√	√	√		√
Sparsity			√	√	√	√	√
Dynamics	√	√		√	√	√	√
Scalability				√	√		
Confidence	√			√	√	√	
Security	√		√	√	√	√	√
Privacy		√	√	√		√	
Robustness			√				

the event related with the data has taken place or not. Golle et al. (2004) present an approach to maintain a model of VANET at every node. This model contains all the knowledge that a particular node has about the VANET. Incoming information can then be evaluated against the peer's model of VANET. If all the data received agrees with the model with a high probability then the peer accepts the validity of the data.

Three combined trust models have been proposed to model the trustworthiness of peers and use the modeling results to evaluate the reliability of data. Dotzer et al. (2005) suggest building a distributed reputation model that exploits a notion called opinion piggybacking where each forwarding peer (of the message regarding an event) appends its own opinion about the trustworthiness of the data. They provide an algorithm that allows a peer to generate an opinion about the data based on aggregated opinions appended to the message and various other trust metrics including direct trust, indirect trust, and sender based reputation level and Geo-Situation oriented reputation level. Patwardhan et al. (2006) propose an approach in which the reputation of a node is determined by data validation. In this approach, a few nodes, which are named as anchor nodes here, are assumed to be pre-authenticated, and thus the data they provide are regarded as trustworthy. Data can be validated by either agreement among peers or direct communication with an anchor node. Chen et al. (2010b) propose a trust-based message propagation and evaluation framework in vehicular ad-hoc networks where peers share information regarding road condition or safety and others provide opinions about whether the information can be trusted. More specifically, the trust-based message propagation model collects and propagates peers' opinions in an efficient, secure and scalable way by dynamically controlling information dissemination. The trust-based message evaluation model allows peers to evaluate the information in a distributed and collaborative fashion by taking into account others' opinions. Compared to the model of Dotzer et al. (2005), the framework of Chen et al. (2010b) also controls the spread of malicious messages, in order to increase network scalability

Table 1 summarizes and compares the properties that the above mentioned trust models for VANETs can achieve. From this table, we can conclude that none of the trust models has achieved all the desired properties proposed earlier.

FUTURE RESEARCH DIRECTIONS

In this section, we suggest a few important future research directions towards effective trust management for VANETs.

Improving Robustness of Trust Models

Table 1 indicates that robustness has not been paid much attention by researchers in the field of trust management for VANETs. However, for life-critical applications of VANET, it is important for trust models to be robust against various attacks. Some researchers in the general area of trust and reputation systems have recently studied different types of attacks and the robustness of the existing trust and reputation systems (Josang, 2009; Hoffman et al., 2009). The work of Fung et al. (2011) on trust management for collaborative intrusion detection networks has started addressing some of the attacks. Researchers in the field of trust management for VANETs can start from those studies but also consider the unique properties of VANET environments.

Integrating Vehicle to Infrastructure Communication

Existing trust management methods make use of only V2V communications, which are fully distributed. Available infrastructures of VANETs may also be helpful as they provide functionalities of centric collecting, computation and distribution of trust related evidence and results. For example, roadside units may be used to collect local information, filter out false information and share truthful information with vehicles passing by.

For cities with an advanced public transportation system, buses and subways cover almost everywhere. They are running in fixed routes and can serve as a moving infrastructure for VANETs by equipping them with communication and computation devices. Vehicles can communicate with them to provide and acquire up to date local information. Incorporating this type of communication may increase system scalability and cope with the sparsity problem. One way to integrate them may be to rely on the super-agent based reputation management method as proposed in the work of Wang et al. (2010a, 2010b) by treating buses and subways as super-peers in the network.

Interacting with the Networking Layer

Built for the application layer, most of the existing trust management methods for VANETs do not concern much about the networking layer. However, the design of trust management methods is limited by the networking layer design, such as communication range, routing protocols, and existence of infrastructure. It is thus worthwhile to investigate effective trust management in the application layer by interacting with the networking layer.

Effective trust management method cannot be designed without the consideration of existing routing protocols. As messages are disseminated according to routing protocols, messages about events happening, trust opinions about the messages and reputation information of other peers have to be distributed in a certain designed manner. Understanding the advances of routing protocols will help the design of effective trust management. For example, the trust-based message propagation and evaluation framework proposed in the work of Chen et al. (2010a, 2010b) makes use of a cluster-based routing scheme for the evaluation of messages sent by peers and the update of peers' trustworthiness. More specifically, peer vehicles in a VANET are grouped into multiple clusters. Messages shared by peers regarding road condition or safety are sent to cluster leaders and distributed to their cluster members. Upon receiving the messages, the leaders send the messages to their cluster members, collect evaluation of messages from the members, and compute the trust of the messages based on aggregated evaluation. This information will be useful for vehicles to decide whether to follow the messages. The trust model designed based on the cluster-based routing scheme has been evaluated to be quite effective under the pervasive presence of false information. At the same time, the computed trust of messages can be used to enhance the routing protocol. More specifically, the cluster

leaders in the system also make decisions on whether to further relay the messages based on the computed trust of the messages. In this way, malicious messages or spam get controlled, and network scalability is much improved. For future directions, it is worthwhile to look into other advanced routing protocols that may give valuable hints in the design of the effective trust management, and how the results of trust management can be useful for improving and securing those routing protocols.

Reputation Scheme

Incorporating reputation information in trust management can effectively cope with the sparsity problem where no reliable trust information exists for vehicles in a certain small area within communication ranges. However, deploying a reputation management model in VANETs is a challenging task given the highly distributed nature of VANET environments. And, the vehicles are constantly roaming around. There is no enough time for a vehicle to communicate with the central server to acquire reputation information of another vehicle.

One possible direction to look into is the Pretty Good Privacy (PGP) Web of Trust widely accepted as the first successful attempt to make cryptography freely available to the public (Abdul-Rahman, 1997). The idea is that PGP Web of Trust does not rely on a trusted authority to cryptographically create a trusted digital certificate to specify the real owner of a public key. Instead, it allows the user who has a private key to create a digital certificate for the corresponding public key. To address the issue where the user may specify an arbitrary (unreal) owner for the public key in the certificate, PGP Web of Trust allows other users to digitally sign certificates that they believe to be authentic, i.e., the specified owner in the certificate is indeed the real owner of the public key. A user can verify a public key by checking whether there are digital signatures signed by other users whom she trusts. A similar idea of PGP Web of Trust may be adopted to allow each peer vehicle to specify whether other peer vehicles can be trusted based on the peer's own experience. This information can then be used by others to decide whether to trust the vehicles.

One limitation about PGP Web of Trust is that it makes use of only direct trust relationships between users. To be more specific, only when a digital signature is signed by other users whom the user directly trusts, the user will believe the certificate to be authentic. In other words, PGP does not consider the transitivity property of trust. To overcome the shortcoming, a trusted neighborhood expansion approach has been proposed in Guo et al. (2011). This approach first merges the feedbacks on certificates provided by trusted neighbors of an active user, which may include both directly trusted neighbors specified by the user (including herself because the user should trust herself) and indirectly trusted ones identified by trust propagation used in the extended PGP Web of Trust. By relying on the majority opinion and ensuring the high consistency among the feedbacks, the merged feedback set can then well represent the opinions of this active user. Based on the merged feedback set, the method then finds other similar users of the active user who are not in the original trusted neighborhood. In this way, the trusted neighborhood is further expanded. The similar problem may also exist in VANETs because of the potentially large population of vehicles in the environment. It is often that peers do not directly trust the others that specified their trust on some particular vehicles. Thus, the trusted neighborhood expansion approach may also be applied in VANETs to find more trustworthy vehicles that are not directly trusted by peer vehicles.

Leveraging Social Network of Passengers

To improve the capability of coping with sparsity, trust models may take into account social network information of passengers retrieved from social networking sites such as Facebook, Twitter and etc. Passengers in the system can also directly specify their trust on and relationship with others. Based on the

obtained social network information, a unified social network of passengers can be built and maintained. Each passenger is a node in the social network and connected by directed links. A directed link from one passenger to another means that the former passenger trusts the latter one with a certain level because the latter has a particular relationship with the former in the social network. The weight of the link represents how much the trust is. Carefully applying the transitivity property of trust (Mui et al., 2002), a passenger's trust on others who are not directly connected can be computed. In this way, the rich information about passengers' social networks can be utilized.

Development of a Comprehensive Simulation Framework

Real-life experiments can be difficult and expensive to implement because of the dire consequences of mistakes/inaccuracy (i.e., involved human subjects being injured or even killed), the high number of vehicles and real-life scenarios involved. It is difficult to perform actual empirical performance measurement also because of the inherently distributed and complex VANET environments. To overcome these limitations, VANET simulation frameworks should be used extensively.

Existing VANET simulators are either traffic simulators (Choffnes & Bustamante, 2005) or network simulators (Zeadally et al., 2010). Traffic simulators are used for transportation and traffic engineering to simulate traffic and road conditions. Network simulators are used for evaluating network protocols and applications. A comprehensive VANET simulator needs to integrate these two types of simulators together in an interactive manner. Moreover, there does not exist a VANET simulator that is specifically designed for evaluating and comparing trust management methods.

Most of the evaluation frameworks for trust management in VANETs are built based on the ns2 simulator that is a network simulator or the SWANS (Scalable Wireless Ad-hoc Network Simulator) that is a traffic simulator. These evaluation frameworks lack flexibility in integrating various real-life scenarios, and thus are difficult to verify the properties of trust management (Zeadally et al., 2010). For example, the traffic and network simulators do not concern about the types and actual content of the messages distributed across the network and among all peer vehicles. The actual content of messages is however very important for trust management as trust evaluation of a peer is dependent on the truthfulness or quality of message content passed by the peer. More sophisticated cheating behaviors of peers should also be simulated by these evaluation frameworks so that the robustness of trust management can be extensively tested.

CONCLUSION

In conclusion, in this article, we clearly point out the challenges in VANET environments, and identify a list of important properties that should be achieved by trust management for VANET, setting a clear goal for researchers in this area. We also show the lack of effectiveness of the existing trust models for VANET, draw particular attention to the robustness of trust models, and suggest some important future directions. Our research thus serves as one step closer towards the design and development of effective trust management for the deployment of safety, life-critical and road condition related systems by governments and business organizations to enhance road safety and reduce the number of car accidents and traffic congestion.

REFERENCES

Abdul-Rahman, A. (1997). The pgp trust model. *EDI-Forum: The Journal of Electronic Commerce*, *10*(3), 27–31.

Balakrishnan, V., Varadharajan, V., & Tupakula, U. (2008). Subjective logic based trust model for mobile ad hoc networks. In *Proceedings of the International Conference on Security and Privacy in Communication Networks*.

Chen, C., Zhang, J., Cohen, R., & Ho, P. H. (2010a). Secure and efficient trust opinion aggregation for vehicular ad-hoc networks. In *Proceedings of the IEEE 72nd Vehicular Technology Conference* (pp. 1-5).

Chen, C., Zhang, J., Cohen, R., & Ho, P. H. (2010b). A trust-based message propagation and evaluation framework in vanets. In *Proceedings of the International Conference on Information Technology Convergence and Services*.

Choffnes, D. R., & Bustamante, F. E. (2005). An integrated mobility and traffic model for vehicular wireless networks. In *Proceedings of the International Workshop on Vehicular Ad Hoc Networks* (pp. 69-78).

Dellarocas, C. (2000). Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In *Proceedings of the ACM Conference on Electronic Commerce* (pp. 150-157).

Dotzer, F., Fischer, L., & Magiera, P. (2005). Vars: A vehicle ad-hoc network reputation system. In *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* (pp. 454-456).

Douceur, J. (2002). The sybil attack. In *Proceedings of the First International Workshop on Peer-to-Peer Systems*.

Eichler, S., Schroth, C., & Eberspacher, J. (2006). Car-to-car communication. In *Proceedings of the VDE-Kongress: Innovations for Europe*.

Elbatt, T., Goel, S. K., Holland, G., Krishnan, H., & Parikh, J. (2006). Cooperative collision warning using dedicated short range wireless communications. In *Proceedings of the International Workshop on Vehicular Ad Hoc Networks* (pp. 1-9).

Fung, C., Zhang, J., Aib, I., & Boutaba, R. (2011). Dirichlet-based trust management for effective collaborative intrusion detection Networks. *IEEE Transactions on Network and Service Management*, *8*(2), 79–91. doi:10.1109/TNSM.2011.050311.100028

Gerlach, M. (2007). Trust for vehicular applications. In *Proceedings of the International Symposium on Autonomous Decentralized Systems* (pp. 295-304).

Golle, P., Greene, D., & Staddon, J. (2004). Detecting and correcting malicious data in vanets. In *Proceedings of the International Workshop on Vehicular Ad Hoc Networks* (pp. 29-37).

Guo, G., Zhang, J., & Vassileva, J. (2011). Improving pgp web of trust through the expansion of trusted neighborhood. In *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence* (pp. 489-494).

Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys*, *42*(1), 1–31. doi:10.1145/1592451.1592452

Huynh, T., Jennings, N., & Shadbolt, N. (2006). An integrated trust and reputation model for open multi-agent systems. *Autonomous Agents and Multi-Agent Systems*, *13*(2), 119–154. doi:10.1007/s10458-005-6825-4

Jøsang, A., & Golbeck, J. (2009). Challenges for robust of trust and reputation systems. In *Proceedings of the 5th International Workshop on Security and Trust Management*.

Jøsang, A., & Ismail, R. (2002). The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference* (pp. 324-337).

Leckie, C., & Kotagiri, R. (2003). Policies for sharing distributed probabilistic beliefs. In *Proceedings of the 26th Australasian Computer Science Conference* (Vol. 16).

Li, F., & Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, *2*(2), 12–22. doi:10.1109/MVT.2007.912927

Mass, Y., & Shehory, O. (2001). Distributed trust in open multi-agent systems. In R. Falcone, M. Singh, & Y.-H. Tan (Eds.), *Proceedings of the Conference on Trust in Cybersocieties* (LNCS 2246, pp. 159-173).

Minhas, U. F., Zhang, J., Tran, T., & Cohen, R. (2010a). Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modeling based on direct experience with incentives for honesty. In *Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology* (pp. 243-247).

Minhas, U. F., Zhang, J., Tran, T., & Cohen, R. (2010b). Towards expanded trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence Theory and Practice*, *5*(1).

Minhas, U. F., Zhang, J., Tran, T., & Cohen, R. (2011). A multi-faceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. *IEEE Transactions on Systems, Man and Cybernetics. Part C, Applications and Reviews*, *41*(3), 407–420. doi:10.1109/TSMCC.2010.2084571

Mui, L., Mohtashemi, M., & Halberstadt, A. (2002). A computational model of trust and reputation. In *Proceedings of the 35th Hawaii International Conference on System Science* (pp. 2431-2439).

Nadeem, T., Dashtinezhad, S., Liao, C., & Iftode, L. (2004). Trafficview: Traffic data dissemination using car-to-car communication. *ACM Mobile Computing and Communications Review*, *8*(3), 6–19. doi:10.1145/1031483.1031487

Patwardhan, A., Joshi, A., Finin, T., & Yesha, Y. (2006). A data intensive reputation management scheme for vehicular ad hoc networks. In *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems* (pp. 1-8).

Poslad, S., Calisti, M., & Charlton, P. (2002). Specifying standard security mechanisms in multi-agent systems. In *Proceedings of AAMAS Workshop on Deception, Fraud and Trust in Agent Societies* (pp. 163-176).

Rahman, S., & Hengartner, U. (2007). Secure vehicle crash reporting. In *Proceedings of the International Conference on Mobile Computing*.

Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*, 39–68.

Raya, M., Papadimitratos, P., Gligor, V., & Hubaux, J. (2008). On data-centric trust establishment in ephemeral ad hoc networks. In *Proceedings of the IEEE Conference INFOCOM* (pp. 1238-1246).

Regan, K., Poupart, P., & Cohen, R. (2006). Bayesian reputation modeling in e-marketplaces sensitive to subjectivity, deception and change. In *Proceedings of the Conference on Artificial Intelligence* (pp. 1206-1212).

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM*, *43*(12), 45–48. doi:10.1145/355112.355122

Sabater, J., & Sierra, C. (2001). Regret: A reputation model for gregarious societies. In *Proceedings of the AAMAS Workshop on Deception, Fraud and Trust in Agent Societies* (pp. 475-482).

Staab, E., Fusenig, V., & Engel, T. (2008). Towards trust-based acquisition of unverifiable information. In *Proceedings of the 12th International Workshop on Cooperative Information Agents* (pp. 41-54).

Teacy, W., Patel, J., Jennings, N. R., & Luck, M. (2006). TRAVOS: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems*, *12*(2), 183–198. doi:10.1007/s10458-006-5952-x

Tran, T. (2005). A reliability modelling based strategy to avoid infinite harm from dishonest sellers in electronic marketplaces. *Journal of Business and Technology*, *1*(1), 69–76.

Wang, Y., & Singh, M. P. (2007). Formal trust model for multiagent systems. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence.*

Wang, Y., Zhang, J., & Vassileva, J. (2010a). Effective web service selection via communities formed by super-agents. In *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence* (pp. 546-556).

Wang, Y., Zhang, J., & Vassileva, J. (2010b). Super-agent based reputation management with a practical reward mechanism in decentralized systems. In *Proceedings of the IFIP International Conference on Trust Management.*

Wex, P., Breuer, J., Held, A., Leinmuller, T., & Delgrossi, L. (2008). Trust issues for vehicular ad hoc networks. In *Proceedings of the 67th IEEE Vehicular Technology Conference* (pp. 2800-2804).

Wikipedia. (n.d.). *Road traffic safety*. Retrieved from http://en.wikipedia.org/wiki/Road_traffic_safety

Wu, D. J., & Sun, Y. (2001). The emergence of trust in multi-agent bidding: a computational approach. In *Proceedings of Hawaii International Conference on System Sciences*.

Xu, Q., Mak, T., Ko, J., & Sengupta, R. (2004). Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the International Workshop on Vehicular Ad Hoc Networks*.

Yu, B., & Singh, M. (2000). A social mechanism of reputation management in electronic communities. In *Proceedings of the 4th International Workshop on Cooperative Information Agents* (pp. 154-165).

Yu, B., & Singh, M. (2002a). Distributed reputation management for electronic commerce. *Computational Intelligence*, *18*(4), 535–549. doi:10.1111/1467-8640.00202

Yu, B., & Singh, M. (2002b). An evidential model of distributed reputation management. In *Proceedings of International Autonomous Agents and Multi Agent Systems* (pp. 294-301).

Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2010). Vehicular ad hoc networks (vanets): Status, results, and challenges. *Telecommunication Systems*, *51*(2), 1–25.

Zhang, J. (2011). A survey on trust management for vanets. In *Proceedings of the 25th International Conference on Advanced Information Networking and Applications* (pp. 105-112).

Zhang, J., & Cohen, R. (2008). Evaluating the trustworthiness of advice about selling agents in e-marketplaces: A personalized approach. *Electronic Commerce Research and Applications*, *7*(3), 330–340. doi:10.1016/j.elerap.2008.03.001

Zhang, J., Sensoy, M., & Cohen, R. (2008). A detailed comparison of probabilistic approaches for coping with unfair ratings in trust and reputation systems. In *Proceedings of the 6th Annual Conference on Privacy, Security and Trust* (pp. 189-200).

Jie Zhang is currently an Assistant Professor at the School of Computer Engineering, Nanyang Technological University, Singapore. He received the Ph.D. degree from the University of Waterloo, Canada, in 2009, and was the recipient of the Alumni Gold Medal awarded once a year to honour the top PhD graduate. His research interests include artificial intelligence, multi-agent systems, trust modelling, incentive mechanisms, and vehicular ad hoc networks. His papers have been published by top journals (i.e. Computational Intelligence) and conferences (i.e. AAAI, AAMAS, WI and UMAP). He has also won 4 best paper awards at CNSM'10, IM'09, ITCS'10 and CSWWS'06. He is also active in serving research communities as co-chair for TRUM'11, publication and publicity chair for PST'10, associate editor for ICIS'10, PC members for AAMAS'11, AAAI'10, and reviewers for JAAMAS, Computational Intelligence, etc.