2011 International Conference on Advanced Information Networking and Applications

A Survey on Trust Management for VANETs

Jie Zhang
School of Computer Engineering, Nanyang Technological University, Singapore, zhangj@ntu.edu.sg

***Abstract*—There is an urgent need of effective trust management for vehicular ad-hoc networks (VANETs), given the dire consequences of acting on false information sent out by malicious peers in this context. In this paper, we first discuss the challenges for trust management caused by the important characteristics of VANET environments. We then survey existing trust models in multi-agent systems, mobile ad-hoc networks (MANETs) and VANETs, and point out their key issues. Based on these studies, we suggest desired properties towards effective trust management in VANETs, setting up clear goals for researchers in this area.**

I. 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 [1]. 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.

Network-On-Wheels (NOW) project [2], GST, PreVent and Car-to-Car Consortium [3] 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 [4]. Similar prototypes by other car manufacturers are currently in the testing phase, scheduled to hit the markets over the coming years.

Tremendous effort has also been spent on the development of life-critical or road condition related systems, such as traffic view systems [5], safety message sharing [6], cooperative collision avoidance [7], and secure crash reporting [8]. 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 who 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.

In this paper, we first discuss the challenges for trust management caused by the the large, decentralized, open, sparse and highly dynamic nature of VANET environments. We then comprehensively study the existing trust models in multi-agent systems, mobile and vehicular ad-hoc networks, and summarize their key issues. From these studies, we identify some key desired properties that trust management should incorporate, setting up clear goals for researchers in this area. For each of these properties, we also extensively discuss some potential solutions and the related work that may provide us useful hints, towards effective trust management.

II. 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 kilometers an 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 some of which include network congestion - since vehicles are communicating on a shared channel, information overload - resulting from vehicles receiving a lot of data from the nearby vehicles in a congested area etc. Hence there will be a need to have intelligent vehicle communication systems that are *scalable* and can detect and respond to these potentially hazardous situations by effectively deciding with which peers to communicate [9].

Another key challenge in modeling trust in a VANET environment 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 [10]. Therefore, it is not possible to rely on mechanisms that require a centralized

1550-445X/11 $26.00 © 2011 IEEE
DOI 10.1109/AINA.2011.86

system (e.g. the Centralized Certification Authority and the Trusted Third Party etc) or social networks to build long-term relationships. And in such an environment, there is much *uncertainty* in deciding whom to trust.

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.

III. Existing Trust Models

We survey existing trust models proposed for multi-agent systems, and mobile and vehicular ad-hoc networks. We also point out their key issues when facing the challenges in the VANET domain identified in the previous section.

A. Trust Models in Multi-agent Systems

There is rich literature of trust models in multi-agent systems. Here, we do not provide a summary for each individual model, but discuss specific key issues, each with a set of trust models. For more comprehensive surveys of trust models in multi-agent systems, refer to [11], [12] and [13].

1) Trust Emerging from Multiple Direct Interactions between Agents: Many trust models proposed in multi-agent systems have an underlying assumption that agents interact multiple times with each other over a period of time. In learning and evolutionary models of trust such as those presented in [14], [15], [16], [17], [18], [19], an agent learns to trust (or distrust) another agent based on its past interactions with another agent. If the past interactions with a particular agent have been particularly rewarding, the other agent would then learn to associate a higher trust value resulting in a higher chance of future interactions with this agent. On the other hand, if a certain agent is known to defect over the past interactions, the other agent will choose not to deal with it in the future thus representing a lower (learned) value of trust. In these models, having multiple direct interactions among agents is the key to establishing trust and in learning to evolve strategies over time. However, in highly dynamic and open environments such as VANETs, it is not logical to expect that this assumption will hold. Therefore, the trust models whose success depends on a certain minimum number of direct interactions between the agents, fail when directly applied to the domain of VANETs.

2) Degree of Knowledge about the Environment: Majority of the learning models of trust presented in the literature for multi-agent systems such as [14], [15], [20], [17], assume complete information about other agents and the system (e.g., strategies, payoff matrix etc.) in order to make their trust learning algorithms work. This assumption might hold in certain restrained scenarios (such as controlled simulations) but is simply not true in VANETs where agents are inherently limited in their capacity to gather information from other agents or the environment. Though this issue arises in any multi-agent environment where there is some degree of uncertainty about other agents and the environment, we believe that it is of far more concern in the domain of trust for VANETs and we also attribute it to the rapidly changing dynamics of the agents/environment in the context of VANETs.

3) Role of Central Entities: Some of the reputation models [18] and security mechanisms depend on a central entity (or authority) to gather and aggregate opinions or to authenticate an agent based on a certificate from a central Certification Authority (CA). However, in a decentralized open system such as VANETs, the assumption to have a central authority that is accessible to and trusted by all the peers will not hold. Trust establishment should be decentralized to be applicable to the highly dynamic and distributed environment of VANETs [21], [22], [23]. Even if for a moment we assume that we can implement a central certification authority that overlooks all the peers present in the VANET, given the number of peers expected to be present in the network, the certification list will grow to the extent that authenticating a peer by consulting this central authority (i.e., searching the list of certificates) in real-time would become infeasible not to mention that some models require consulting multiple authorities.

4) Collusion and Strategic Lying: 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. [24]) are vulnerable to strategic lying and collusion.

B. Trust Models in MANETs

As one of the applications of mobile ad-hoc networks, VANETs share some common properties with MANETs, such as decentralization, mobility, openness, and so on. However, there are also differences between them. VANETs are often much larger that may contain millions of vehicles. The network traffic overhead could be high in such a dense VANET environment. The topology of VANETs changes rapidly, since vehicles move fast. A variety of trust models have been proposed in mobile ad-hoc networks. A survey on trust management for MANETs can be found in [25], [26]. The proposed methodologies in [27], [28], [29], [30], [31], [32] target the common goal of reliable packet delivery from the perspective of source routing in mobile ad-hoc networks. In vehicular networks, similar attempts to apply trust to routing may achieve little success in that most of the proposed source routing algorithms in mobile ad-hoc networks do not work well in vehicular networks, plus the fact that trust establishment is more challenging in the vehicle environment.

More specifically, one underlying assumption of many trust models in MANETs is that trust values are always available before a route can be established. In practice, however, trust cannot be established, maintained or retrieved unless a reliable route is available, which is also one important reason why trust is hard to establish in a highly dynamic VANET environment.

Most of the trust models in MANETs deal with the sparsity problem when modeling the trustworthiness of nodes by

collecting trust evidence about them from other nodes in the network, and possibly through some intermediate nodes. This is difficult to be done in VANETs because a VANET environment is often very large and searching for required trust evidence may become impossible given the limited time for decision making.

The goal of trust management in VANETs is not limited to reliable package delivery. One main aim of VANETs is to increase road safety and reduce traffic congestion by allowing information sharing among peers about road and traffic conditions. Trust management in VANETs should help peers detect false information provided by malicious nodes and make informed driving decisions. Trust management in this case is more challenging than that for reliable package delivery. Much dynamics has to be taken into consideration, such as the time and location of reported events, and the types of the events. Thus, previous trust modeling endeavors in mobile ad-hoc networks become worthless when being directly applied to vehicular ad-hoc networks.

C. 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 point out their issues. Note that great efforts, for example the work in [33], [34], 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. A more extensive summary of this kind of trust systems can be found in [35]. We focus on trust models that do not fully rely on the static infrastructure and thus can be more easily deployed. In these models, peers may form trust relationships with each other based on, for example, past interaction experience. They may also gather environmental information about messages sent by other peers to determine the correctness of the data. 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 put more emphasis on evaluating the trustworthiness of data. In these models, normally, no long-term trust relationships between peers will be formed. Combined trust models make extensive use of peer trust to evaluate the trustworthiness of data, but at the same time maintain peer trust over time.

1) Entity-oriented Trust Model: Two typical entity-oriented trust models are the sociological trust model proposed by Gerlach [36] and the multi-faceted trust management model proposed by Minhas et al. [37]. 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 – which depends on situation only, dispositional trust – which is the level of trust based on a peer's own beliefs, system trust – depends on the system and finally belief formation process – which is the evaluation of data based on previous factors. Additionally, they have presented an architecture for securing vehicular communication and a model for preserving location privacy of the vehicle. However, Gerlach does not provide formalization of the architecture about how to combine the different types of trust together. The multi-faceted trust management model of Minhas et al. [37] features in the role-based trust and experience-based trust as the evaluation metric for the integrated trustworthiness of vehicular entities. This model also allows a vehicular entity to actively inquire about an event by sending requests to other entities but restrict the number of reports that are received. For this purpose, the authors introduce in the research the concept of priority-based trust, which provides for an ordering of the value of an information source within a role category, using the influence of experience-based trust. The limit on the number of sources consulted is sensitive to the task at hand. In the end, the trust of information sources and the contextual information about the event such as time and location are integrated into a procedure for gauging whether majority consensus has been reached, which ultimately determines the advice a vehicular entity should follow. The above two trust models have some components in common, for example, situational trust can be compared with event/task specific trust, similarly dispositional trust can be compared to experience or role-based trust. One problem about the multi-faceted trust management is that robustness has not been extensively addressed.

2) Data-oriented Trust Model: In contrast to the traditional view of entity-oriented trust, Raya et al. [38] propose that data-oriented trust may be more appropriate in the domain of Ephemeral Ad-hoc Networks such as VANETs. Data-centric trust establishment deals with evaluating the trustworthiness of the data reported by other entities rather than trust of the entities themselves. In their model, they define various trust metrics of which *a priori* trust relationships in entities is just one of the default parameters and depends on the attributes associated with a particular type of node. Using Bayesian inference and Dempster-Shafer Theory, 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 the event related with the data has taken place or not. Raya et al. also propose the use of task/event specific trust metrics as well as time and location closeness. One of the shortcomings of their work is that trust relationships in entities can never be formed, only ephemeral trust in data is established, and because this is based on a per event basis, it needs to be established again and again for every event. This will work so long as there is enough evidence either in support of or against a specific event, but in the case of data sparsity their model would not perform well.

Golle et al. [39] present a technique that aims to address the problem of detecting and correcting malicious data in VANETs. The key assumption of their approach is in maintaining 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. However, in the case of receiving data which is inconsistent with the model, the peer relies on a heuristic that

tries to restore consistency by finding the simplest explanation possible and also ranks various explanations. The data that is consistent with the highest ranking explanation(s) is then accepted by the node. The major strength of this approach is that it may provide security against adversaries that might even be highly trusted members in the network or might be colluding together to spread malicious data. However, one strong assumption of this approach is that each vehicle has the global knowledge of the network and solely evaluates the validity of data, which may not be feasible in practice.

3) Combined Trust Model: Three combined trust models have been proposed to model trustworthiness of peers and use the modeling results to evaluate the reliability of data. Dotzer et al. [21] have suggested 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, sender based reputation level and Geo-Situation oriented reputation level. This last trust metric allows their model to introduce some amount of dynamism in the calculation of trust by considering the relative location of the information reporting node and the receiving node. Additionally, the situation oriented reputation level allows a node to consider certain situational factors e.g. familiarity with the area, rural or metropolitan area etc. again introducing some dynamism in trust evaluation based on context. One problem is that the authors did not provide sufficient and complete details about the approach. Although they mention that sender based reputation information is managed, they did not describe its formalization or how reputation information can be updated. A more important problem about this approach is that it repeatedly makes use of the opinions from different nodes. The nodes that provide opinions about a message earlier will have larger influence than the nodes generated opinions later, because the earlier nodes' opinions will be repeatedly and recursively considered by later nodes.

Patwardhan et al. [40] 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. Malicious nodes can be identified if the data they present is invalidated by the validation algorithm. One problem about this scheme is that it does not make use of reputation of peers when determining the majority consensus. The majority consensus works well only when a sufficient number of reports about the same event are provided. However, this scheme only passively waits for reports from other peers.

Overcoming some problems of the above two models, Chen et al. propose a trust-based message propagation and evaluation framework in vehicular ad-hoc networks [41] 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. This model is demonstrated to promote network scalability and system effectiveness in information evaluation under the pervasive presence of false information, which are the two essentially important factors for the popularization of VANETs.

IV. Desired Trust Management for VANET

Based on our studies on the challenges in VANET environments and the existing trust models in different domains, we propose here a list of desired properties that effective trust management should incorporate for VANETs.

A. Decentralized Trust Establishment

Trust establishment should be fully decentralized to be applicable to the highly dynamic and distributed environment of VANETs [21], [22], [42]. Many trust models such as [19], [37], [43], 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 [23], [44], [42], 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 [45] to collect such information. The models of [23], [44], [42] 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 such as [38], [24], [46], [37], [43] 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 [22] 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.

B. Coping with Sparsity

Effective trust establishment should not be contingent upon a minimum threshold for direct interactions. As described in Section II, 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 [38], [24], [46], [37], [43] can distinguish trustworthy peers from untrustworthy 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 [47], [48] 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.

C. 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 [38], [21]. 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 [49].

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, [39] has 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 [24] 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.

D. 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 [37]. 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 [45], [48]. 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 [41] 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. [48] 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.

E. 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 [46], [50], [15]. In particular, [46] introduced FIRE, a framework that integrates direct trust and role-based trust, in which the direct trust model of [24] 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 modeling the dimensional trust. Wang and Singh [51] 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 peers. Certainty decreases when conflict among reports increases. Balakrishnan et al. [32] express the notion of ignorance during the establishment of trust relationships between mobile nodes. 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 [41].

F. 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 a peer can be uniquely identified. To this end, certain security requirements identified to be essential for trust have been identified in [52], which 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.

G. 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 [53]. 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.

H. 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.

1) Sybil Attack: This type of attacks occurs when a malicious peer in the system creates a large amount of pseudonyms (fake identities) [54]. 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.

2) Newcomer Attack: These attacks occur when a malicious peer can easily register as a new user [55]. 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.

3) Betrayal Attack: Such 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 [19], 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 [56], [18], [45], 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.

4) Inconsistency Attack: These 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. [57]. It can also be coped with by setting time windows and employing a forgetting factor to assign less weight to older experiences.

5) Bad-mouthing/Ballot Stuffing Attack: Reputation systems allow peers to provide feedback about other peers. As pointed by Dellarocas [56], some peers may provide unfairly high feedback to increase others' reputations, which is often referred as "ballot stuffing". Some peers may provide unfairly low feedback to decrease others' reputations, which is often referred as "bad-mouthing". Approaches such as Cluster Filtering of [56], Iterated Filtering of [58] and the personalized approach of [18] have been proposed to address these attacks.

6) Collusion Attack: This type of attacks has been discussed in Section III-A4, and 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.

V. Discussion and Conclusion

In the previous section, we discuss extensively the properties desired by trust management in VANETs given the challenges identified in this environment and the studies on existing trust models in different contexts. Now, we revisit the trust models proposed for VANETs that were surveyed in Section III-C, and summarize and compare the properties they can archive in Table I. From this table, we can conclude that none of the trust models has archived all the desired properties. In particular, robustness has not been paid much attention by researchers in this field. For life-critical applications of VANET, it is important for trust models to be robust against various attacks discussed in Section IV-H and by others (i.e. [59]).

TABLE I
Properties of the Existing Trust Models for VANET

Approaches	[60]	[21]	[39]	[37]	[41]	[36]	[40]
Decentralized	√	√	√	√	√		√
Sparsity			√	√	√	√	√
Dynamics	√	√		√	√	√	√
Scalability				√	√		
Confidence	√			√	√	√	
Security	√		√	√	√	√	√
Privacy		√	√	√		√	
Robustness			√				

In conclusion, this is the first survey on trust management for VANETs. We clearly identify the challenges in this environment, survey existing trust models proposed for different contexts, and point out their issues when being taken to the VANET domain. We propose a list of important properties that should be archived by trust management for VANET, setting a specific goal for researchers in this area. We also show the lack of effectiveness of the existing trust models for VANET, and draw particular attention to the robustness of trust models. 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

[1] "Wikipedia on road traffic safety," *http://en.wikipedia.org/wiki/Road-traffic_safety*.

[2] T. N. on Wheels (NOW) Project, *http://www.network-on-wheels.de/*.

[3] T. C. to Car Communication Consortium (C2CC), *http://www.car-to-car.org/*.

[4] GM, "Threat assessment algorithm," *http://www.nhtsa.dot.gov/people/injury/research/pub/acas/acasest/*.

[5] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode, "Trafficview: Traffic data dissemination using car-to-car communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 8, p. 2004, 2004.

[6] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," in *Proceedings of VANET*, 2004.

[7] T. Elbatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *Proceedings of VANET*, 2006.

[8] S. Rahman and U. Hengartner, "Secure vehicle crash reporting," in *Proceedings of MOBICOMM*, 2007.

[9] C. Leckie and R. Kotagiri, "Policies for sharing distributed probabilistic beliefs," in *Proceedings of ACSC*, 2003, pp. 285–290.

[10] S. Eichler, C. Schroth, and J. Eberspacher, "Car-to-car communication."

[11] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, no. 1, pp. 1–25, 2004.

[12] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[13] Y. Wang and J. Vassileva, "Toward trust and reputation based web service selection: A survey," *International Transactions on Systems Science and Applications*, vol. 3, no. 2, pp. 118–132, 2007.

[14] Y. S. D.J. Wu, "The emergence of trust in multi-agent bidding: a computational approach," in *Proceedings of the 34th Hawaii International Conference on System Sciences*, vol. 1, 2001.

[15] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation," in *Proceedings of the 35th Hawaii International Conference on System Science (HICSS)*, 2002.

[16] K. Regan, P. Poupart, and R. Cohen, "Bayesian reputation modeling in e-marketplaces sensitive to subjectivity, deception and change," in *Proceedings of the Conference on Artificial Intelligence (AAAI)*, 2006.

[17] S. Sen, "Reciprocity: A foundational principle for promoting cooperative behavior among self-interested agents," in *Proceedings of the Second International Conference on Multi-Agent Systems*, 1996, pp. 322–329.

[18] J. Zhang and R. Cohen, "Trusting advice from other buyers in e-marketplaces the problem of unfair ratings," in *Proceedings of the Eighth International Conference on Electronic Commerce*, 2006.

[19] T. Tran, "A reliability modelling based strategy to avoid infinite harm from dishonest sellers in electronic marketplaces," *Journal of Business and Technology (JBT)*, vol. 1, no. 1, pp. 69–76, 2005.

[20] R. Mukherjee, B. Banerjee, and S. Sen, "Learning mutual trust," *Trust in Cyber-societies, Springer-Verlag*, pp. 145–158, 2001.

[21] F. Dotzer, L. Fischer, and P. Magiera, "Vars: A vehicle ad-hoc network reputation system," in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2005.

[22] Y. Mass and O. Shehory, "Distributed trust in open multi-agent systems," *Trust in Cyber-societies, Berlin: Springer-Verlag*, pp. 159–173, 2001.

[23] B. Yu and M. P. Singh, "A social mechanism of reputation management in electronic communities," in *Proceedings of the 4th International Workshop on Cooperative Information Agents*, 2000, pp. 154–165.

[24] J. Sabater and C. Sierra, "Regret: A reputation model for gregarious societies," in *Proceedings of the AAMAS Workshop on Deception, Fraud and Trust in Agent Societies*, 2001, pp. 61–69.

[25] V. Balakrishnan, V. Varadharajan, and U. Tupakula, "Trust management in mobile ad hoc networks," in *Handbook of Wireless Ad hoc and Sensor Networks*. Springer, 2009, pp. 473–502.

[26] J.-H. Cho and A. Swami, "Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks," in *Proceedings of the 14th International Command and Control Research and Technology Symposium*, Washington, DC, 2009.

[27] L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks," in *In Proceedings of the Security Protocols Workshop*. Springer-Verlag, 2002, pp. 47–66.

[28] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proceedings of the ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 1–10.

[29] ——, "Robust cooperative trust establishment for MANETs," in *Proceedings of the ACM workshop on Security of ad hoc and sensor networks*, 2006, pp. 23–34.

[30] G. Theodorakopoulos and J. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, Feb. 2006.

[31] Y. L. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006.

[32] V. Balakrishnan, V. Varadharajan, and U. Tupakula, "Subjective logic based trust model for mobile ad hoc networks," in *Proceedings of the international conference on Security and privacy in communication netowrks*, 2008.

[33] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *Proceedings of VANET*, 2009, pp. 89–98.

[34] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[35] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in *Proceedings of the 67th IEEE Vehicular Technology Conference (VTC Spring)*, 2008.

[36] M. Gerlach, "Trust for vehicular applications," in *Proceedings of the International Symposium on Autonomous Decentralized Systems*, 2007.

[37] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," *International Journal of Computational Intelligence Theory and Practice (IJCITP)*, vol. 5, no. 1, 2010.

[38] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," *Technical Report, LCA-REPORT-2007-003*, 2007.

[39] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of VANET*, 2004.

[40] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, Mobiquitous*, 2006, pp. 1–8.

[41] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust-based message propagation and evaluation framework in vanets," in *Proceedings of the Int. Conf. on Information Technology Convergence and Services*, 2010.

[42] B. Yu and M. Singh, "Distributed reputation management for electronic commerce," *Computational Intelligence*, vol. 18, no. 4, pp. 535–549, 2002.

[43] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "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 (IAT)*, 2010.

[44] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proceedings of International Autonomous Agents and Multi Agent Systems (AAMAS), Bologna, Italy*, 2002.

[45] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

[46] T. Huynh, N. Jennings, and N. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Autonomous Agents and Multi-Agent Systems*, vol. 13, pp. 119–154, 2006.

[47] E. Staab, V. Fusenig, and T. Engel, "Towards trust-based acquisition of unverifiable information," in *Proceedings of the 12th international workshop on Cooperative Information Agents XII*, 2008, pp. 41–54.

[48] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Robust and scalable trust management for collaborative intrusion detection," in *Proceedings of the Eleventh IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2009.

[49] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[50] W. Teacy, J. Patel, N. R. Jennings, and M. Luck, "Travos: Trust and reputation in the context of inaccurate information sources," *Auton Agent Multi-Agent Sys*, vol. 12, pp. 183–198, 2006.

[51] Y. Wang and M. P. Singh, "Formal trust model for multiagent systems," in *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI)*, 2007.

[52] S. Poslad, M. Calisti, and P. Charlton, "Specifying standard security mechanisms in multi-agent systems," in *Proceedings of AAMAS Workshop on Deception, Fraud and Trust in Agent Societies*, 2002.

[53] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39–68, 2007.

[54] J. Douceur, "The sybil attack," in *Proceedings of the First International Workshop on Peer-To-Peer Systems (IPTPS)*, 2002.

[55] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Commun. ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[56] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *Proceedings of the ACM Conference on Electronic Commerce (EC)*, 2000, pp. 150–157.

[57] J. Zhang, M. Sensoy, and R. Cohen, "A detailed comparison of probabilistic approaches for coping with unfair ratings in trust and reputation systems," in *Proceedings of the Sixth Annual Conference on Privacy, Security and Trust (PST)*, 2008.

[58] A. Whitby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," *The Icfain Journal of Management Research*, pp. 48–64, February 2005.

[59] J. G. Audun Josang, "Challenges for robust of trust and reputation systems," in *In Proceedings of the 5th International Workshop on Security and Trust Management (STM)*, 2009.

[60] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proceedings of IEEE Infocom*, 2008.