Journal of Trust Management
a SpringerOpen Journal

RESEARCH Open Access

A trust-based framework for vehicular travel with non-binary reports and its validation via an extensive simulation testbed

Robin Cohen[1], Jie Zhang[2*], John Finnson[1], Thomas Tran[3] and Umar F Minhas[1]

*Correspondence:
zhangj@ntu.edu.sg
[2]School of Computer Engineering, Nanyang Technological University, Singapore, Singapore
Full list of author information is available at the end of the article

Abstract

In this paper, we offer an algorithm for intelligent decision making about travel path planning in mobile vehicular ad-hoc networks (VANETs), for scenarios where agents representing vehicles exchange reports about traffic. One challenge that arises is how best to model the trustworthiness of those traffic reports. To this end, we outline an algorithm for effectively soliciting, receiving and analyzing the trustworthiness of these reports, to drive a vehicle□s decision about the path to follow. Distinct from earlier work, we clarify the need for specifying the conditions under which reports are exchanged and for processing non-binary reports, culminating in a proposed algorithm to achieve that processing, as part of the trust modeling and path planning. To validate our approach we then offer a detailed evaluation framework that achieves large scale simulation of traffic, travel and reporting of information, confirming the value of our proposed approach by demonstrating the average speed of vehicles which follow our algorithm (compared to ones that do not). This experimental framework is promoted as a significant contribution towards the goal of evaluating trust algorithms for intelligent decision making in traffic scenarios.

Keywords: Multi-faceted trust modeling; Multiagent systems; VANET; Vehicle routing; Traffic control

Introduction

In this paper, we present a method for exchanging reports between agents in multiagent systems that allows the trustworthiness of peers providing non-binary information to be modeled, as part of an agent?s decision making process. We are motivated by the problem of enabling agents to make travel decisions based on traffic reports received by peers, in a setting of mobile vehicular ad-hoc networks (VANETs). In this environment, maintaining a multi-faceted trust model is of value and our proposal for supporting non-binary reports ultimately integrates each facet of this trust model, in order for an agent to determine which travel path to follow. For example, a non-binary report could indicate a traffic congestion figure, rather than a binary response to a question such as ?Is the traffic heavy?? Our starting point is a model that includes a calculation of the consensus opinion about roads from the majority of agents, but that assumes only binary reports. From here, we sketch algorithms that clarify in greater detail how to support effective communication between the agents in the environment and how this would then dictate the travel decision making of an agent who is receiving traffic reports from peers.

In order to demonstrate the effectiveness of our framework, we introduce a detailed testbed that simulates vehicles traveling in an environment, making path planning decisions based on non-binary traffic reports from peers whose trustworthiness has been modeled. We offer an extensive set of simulations that serve to validate our approach, illustrating how effective the average path time taken by our vehicles is, in comparison with a best case scenario with perfect knowledge and with models that integrate less detailed trust modeling.

The dual contributions are: i) an effective decision making process for intelligent agents in VANET environments where trust is modeled and non-binary reports are exchanged ii) an extensive testbed of use for measuring the value of different trust modeling algorithms, in travel environments where agents exchange reports. We clarify the importance of these contributions in comparison with related work in the field.

Background: multi-faceted trust model

In this section, we outline our original framework for modeling trust in VANET environments ([1-3]). We consider the driver of each vehicle in our VANET environment to be represented by an agent. In order for each vehicle on the road to make effective traffic decisions, information is sought from other vehicles[a] (about the traffic congestion on a particular road). As a result, for each driver an intelligent agent constructs and maintains a model for each of the other vehicles. Travel decisions are then made based on a multi-faceted model of agent[b] trustworthiness. This is necessary because when asked, each agent may report inaccurate traffic congestion, in an effort to deflect other vehicles from certain roads. In particular, we propose a core processing algorithm to be used by each agent that seeks advice (about travel paths, based on traffic) from other vehicles in the environment as summarized below.

Algorithm 1: Computation Steps

```
while on theroad do
    Send requests and receive responses;
    if in need of advice then
        Choose n; //number of agents to ask for advice
        //according to roles and experiences
        Prioritize n agents;
        if response consensus > acceptable ratio then
            Follow advice in response;
        else
            Follow advice of agent with highest role and highest trust value;
    Verify reliability of advice;
    Update agents? trust values;
```

In order to cope with possible data sparsity, various facets (highlighted in this section in bold) of each agent are taken into consideration when reasoning about travel, including the agent?s role, location and inherent trustworthiness (determined on the basis of past experiences with this particular agent - i.e. whether past advice has proven to be trustworthy). Each of these facets of the agent is stored within the trust model.

We first acknowledge that certain vehicles in the environment may play a particular **role** and, on this basis, merit greater estimates of trustworthiness. For example, there may be vehicles representing the police and other traffic authorities (authority) or ones representing radio stations dedicated to determining accurate traffic reports by maintaining vehicles in the vicinity of the central routes (expert). Or there may be a collection of agents representing a ?commuter pool?, routinely traveling the same route, sharing advice (seniority).

Consideration of any past personal **experiences** with agents allows the model to include any learning about particular agents due to previous encounters, specifically modeling trustworthiness each time and adjusting the level of trust to be higher or lower, based on the outcome of the advice that is offered. The equations which adjust experience-based trust are as below:

$$T_A(B) \leftarrow T_A(B) + \alpha(1 \quad T_A(B)) \tag{1}$$

$$T_A(B) \leftarrow T_A(B) + \beta(1 \quad T_A(B)) \tag{2}$$

Experience-based trustworthiness is represented and maintained following the model of [4] where $T_A(B) \in (\quad 1, 1)$ represents A?s trust in$B$ (with -1 for total distrust and 1 for total trust) which is incremented by $0 < \alpha < 1$ using Equation (1) if B?s advice is found to be reliable (positive experience), or decremented by $\quad 1 < \beta < 0$ using Equation (2) if unreliable (negative experience), with $\beta > \alpha$ to reflect that trust is harder to build up but easier to tear down. Distinct from the original model of [4], the values of α and β can be set to be event-specific. For example, when asking about a major accident, these values may be set high, to reflect considerable disappointment with inaccurate advice. We also incorporate a requirement for agents to reveal whether the traffic information they are providing has been directly observed or only indirectly inferred from other reports that agent has received. The critical distinction of direct or indirect reporting then influences the values set for α and β, introducing greater penalties for disappointment with direct advice. In [2] we discuss at greater length the incentives to honesty that are introduced within this framework; for brevity, we omit that discussion in this paper.

A central calculation to influence the travel decision of each agent is the determination of **majority consensus** amongst the agents providing advice about a particular road. The agent maintains, as part of her model of other agents, a list of agents to ask for advice. This list is ordered from higher roles to lower roles with each group G_i of agents of similar roles being ordered from higher experience-based trust ratings to lower ratings. The agent sets a value n and asks the first n agents[c] from her ordered list the question (thus using priority-based trust), receives their responses (reports), and then performs majority-based trust measurement. Suppose that q of these n agents declare that their reports are from direct experience/observation. The requesting agent determines whether there are sufficient direct witnesses such that she can make a decision based solely on their reports.

If $q \geq N_{min}$, then the requesting agent will only consider the reports from the q direct witnesses if a majority consensus on a response can be reached, up to some tolerance set by the requester (e.g. the agent may want at most 30% of the responders to disagree), then the response is taken as the advice and followed. If $q < N_{min}$, then there are insufficient direct witnesses; the agent will consider reports from both direct and indirect witnesses, assigning different weight factors to them, computing and following the majority opinion. (Once the actual road conditions are verified, the requesting agent adjusts the experience-based trust ratings of the reporting agents: It penalizes (rewards) more those agents who reported incorrect (correct) information in the direct experience case than those agents with incorrect (correct) information in the indirect experience case.) If a majority consensus cannot be reached, then instead, the agent relies on role-based trust and experience-based trust (e.g., taking the advice from the agent with highest role and highest experience trust value). Note that in order to eventually admit new agents into consideration, the agent will also ask a certain number of agents beyond the n^{th} one in the list. The responses here will not be considered for decision, but will be verified to update experience-based trust ratings and some of these agents may make it into the top n agents, in this way.

The computation of majority consensus adheres to the set of formulae outlined as follows: Suppose agent A receives a set of m reports $\mathcal{R} = \{R_1, R_2, \ldots, R_m\}$ from a set of n other agents $\mathcal{B} = \{B_1, B_2, \ldots, B_n\}$ regarding an event. Agent A will consider more heavily the reports sent by agents who have higher level roles and larger experience-based trust values. When performing majority-based process, we also take into account the **location** closeness between the reporting agent and the reported event, and the closeness between the **time** when the event has taken place and that of receiving the report. We define C_t (time closeness), C_l (location closeness), T_e (experience-based trust) and T_r (role-based trust). Note that all these parameters belong to the interval $(0, 1)$ except that T_e needs to be scaled to fit within this interval by $(T_e + 1)/2$.

For each agent B_i $(1 \leq i \leq n)$ belonging to a subset of agents $\mathcal{B}(R_j) \subseteq \mathcal{B}$ who report the same report $R_j \in \mathcal{R}$ $(1 \leq j \leq m)$, we aggregate the effect of its report according to the above factors. The aggregated effect $E(R_j)$ from reports sent by agents in $\mathcal{B}(R_j)$ can be formulated as follows [2]:

$$E(R_j) = \sum_{B_i \in \mathcal{B}(R_j)} \frac{T_e(B_i) T_r(B_i)}{C_t(R_j) C_l(B_i) W(B_i)} \tag{3}$$

$W(B_i)$ is a weight factor set to 1 if agent B_i who sent report R_j is an **indirect** witness, and $W(B_i)$ is set to a value in $(0, 1)$ if user B_i is a direct witness[d].

A majority consensus can be reached if

$$\frac{M(R)}{\sum_{R_j \in \mathcal{R}} E(R_j)} \geq 1 \quad \varepsilon \tag{4}$$

where $\varepsilon \in (0, 1)$ is set by agent A to represent the maximum error rate that A can accept and $M(R) = \max_{R_j \in \mathcal{R}} E(R_j)$. A majority consensus can be reached if the percentage of the opinion (the effect among different reports) over all possible opinions is above the threshold set by agent A.

The trust modeling framework described so far clarifies the algorithms that lead to the calculation of the trustworthiness value which would then be stored in each agent model.

Trip planning decisions of a vehicle would then be made in light of these particular agent models. One element that requires further clarification is detailed agent communication protocols to exchange reports. This is elaborated in the section that follows.

Agent communication protocols to exchange reports

The framework in [3] (see also [1,2]) is designed with a pull based communication protocol, where agents send requests to other agents for information. In addition to this classic pull oriented design, we introduce a push based protocol for broadcasting information. These protocols dictate when communication is initiated and to whom. Either or both of the two protocols can be used for communicating information between agents. Algorithm 2 describes the push and pull based protocol and how a priority road information request is sent by agents. This is part of our proposal for specifying when trust modeling should be integrated into the decision making process of these agents.

We note that this algorithm serves to provide important detail and clarification to advance the earlier proposal of [3]. In that work, the messaging proposed was vague. It was suggested that the message content (congestion information about a road) would be a ?yes? or ?no? response to a question ?Is this road congested?? and that this response would be pulled to the requesting agent. When the pulls would occur was left vague as ?in need of advice?. As such, which roads were being investigated was also left unspecified. The concept of a priority road, introduced below, facilitates messaging and serves to provide the clearer specification of communication. Roads are placed into priority for an agent if there is a gap of information about congestion; subsequent to receiving a report about a priority road, that road?s status may be altered to cause it to be removed from the priority list (if sufficient information on that road has accumulated). How agents choose to designate a road as priority can be left as an implementation detail. In the simulations used to validate our model, if road information was empty or was sufficiently old, that road would be added to the priority list.

Algorithm 2: Pull and Push Based Communication

```
while on the road do
    if Triggered according to communication frequency then
        //Pull protocol
        //Get road to request advice about and agent to request from
        if priority road exists then
            Choose highest priority road;
            Get trustworthy agent;
            if Trustworthy agent exists then
                Send request to trustworthy agent for advice concerning the high
                priority road;
            else
                Send request to any agent for advice concerning the high priority road;
        //Push protocol
        //Broadcast current location and congestion to agents
        Broadcast current location and congestion;
```

The pull protocol allows agents (requester) to request information from other agents (requestee). The trustworthiness of the information from the requestee agent is modeled and used to determine what path to follow based on the report produced. On the other hand, the push protocol allows agents to send information to other agents, even if it were not requested. The trustworthiness of the sender agent is still modeled; this may then be employed during decision making about travel paths. Both of these protocols are set to occur according to a certain communication frequency; this is the tactic employed during our simulation of traffic which serves to provide the validation of our proposed framework (see Section ?Simulation results?). Setting the communication to happen fairly frequently allows agents to inquire about any roads for which they lack sufficient guidance and keeps the information flowing between agents, from the push broadcasting.

Three types of messages are supported within our protocol. The three messages are a transmission of an agent?s location and congestion (Location and Congestion Push), a request for congestion information about a specific road (Priority Road Information Pull Request), and a response for congestion information about a specific road (Priority Road Information Pull Response).

We begin with a clarification of how our messaging framework would support trust modeling in the context of Boolean traffic reports. Algorithm 1 theoretically sends requests only to agents in a prioritized list, when advice was needed. Our proposed update to this algorithm, shown in Algorithm 3, would have each agent?s knowledge base continuously updated with periodic messages, from the pull, push or both protocols. When advice is needed, the most relevant and trustworthy reports are chosen and used.

Algorithm 3: New Majority Computation Steps, with Advice Gathering Update

```
while on the road do
    Send requests and receive responses;
    if in need of advice then
        Choose $n$ reports $R$; //number of reports to use for advice
        Check Priority Road(Current Road);//to help update the Priority list
        Prioritize $n$ reports; //according to roles and experiences
        if response consensus > acceptable ratio then
            Follow advice in response;
        else
            Follow advice of agent with highest role and highest trust value;
    Verify reliability of advice;
    Update agents? trust values;
```

The work by Minhas et al. mentioned in Section ?Background: multi-faceted trust model? presented a Multi-faceted Trust Management Framework that was described as operational for Boolean values of congestion (Heavy (True), Light (False)). In order to calculate a majority opinion, reports which featured the same Boolean value of congestion were aggregated together. The percentage of reports with same congestion value would be compared against a threshold to determine whether the advice would be followed. The trust modeling itself respects the formulae outlined in Section ?Background: multi-faceted trust model?. The use of a new advice gathering protocol (as per Algorithm 2) would not intrinsically alter the majority opinion calculation; it simply clarifies how traffic reports are retrieved. Note that calling *Check Priority Road(Current Road)* within this algorithm has the eventual effect of coping with stale or missing information on roads that are critical to current path planning.

Our proposed numeric trust modeling

In this section we clarify how our framework could support the use of numeric traffic reports, leading to a ?confidence metric? used for trust modeling, in contrast to the Boolean evaluation of traffic in Section ?Background: multi-faceted trust model?. Our new proposed confidence metric and use of numeric congestion and trust values serve to allow a more accurate description of traffic and agent information.

The original theory in Section ?Background: multi-faceted trust model? assumed that congestion would be communicated as a simple *true* (Heavy) or *false* (Light), stating either that the road was congested or not. However, direct application may result in an unfair and biased calculation of the majority opinion. This is because determining whether a road is congested or not is a subjective opinion and is prone to inaccuracies. Also, by representing the congestion as a Boolean, this severely limits the system?s ability to compare roads, evaluate agents, and make the best decisions. Our proposed model seeks to alleviate this problem by representing congestion as a number, which will bring a more suitable level of accuracy to the system[e].

Formula (3) shows the calculation for the aggregated effect of a majority opinion. The new way of representing congestion as a numeric value requires a careful recasting of formula (3). (3) aggregates the effect of all agents that sent the same report (i.e. cong = true). This simple aggregation of similar reports is impossible with the new congestion representation because there are no longer only two types of reports (Cong=true or Cong=false). In the new framework, each report must be evaluated for addition into the majority opinion system. This is done by giving the report a confidence and then evaluating it for inclusion into the majority opinion (similar to the aggregated effect calculation).

The following sections will detail how the factors of experience and role based trust, time and location closeness, and whether the advice is direct or indirect are incorporated into our proposed confidence metric and utilized in calculating a majority opinion.

Confidence calculation

Confidence functions as a metric similar to trust, and is calculated by combining many different report and agent factors, which were introduced in Formula (3) and will be described in detail later in this section. These factors include experience and role based trust, time and location closeness, and whether the advice is direct or indirect.

Our proposed equation for calculating confidence must effectively replace Formula (3), while representing a trust-like metric. Modifications to confidence should then be reflected in a manner similar to how trust is increased and decreased in Equations (1) and (2). α and β function in these equations as a standard for increasing and decreasing trust, respectively. For our proposed confidence calculation it did not make sense to atomically increase or decrease the value according to the influencing factor (role, time closeness, etc.). The increase or decrease should reflect the significance of the factor. As a result, our proposed confidence metric replaces Formula (3) with Equation (6), where Equations (1) and (2) are used as the basis for calculating the confidence of report R_j, through a modified summation of a geometric series[f].

The factors of role based trust, time and location closeness, and whether the advice is direct or indirect in Formula (3), are reflected through Variable (G). Each factor is integrated, in turn, yielding an overall *Conf* value. In order to do so, G needs to be calculated, as explained in the subsections that follow[g]. Experience based trust of an agent automatically forms the default value of the confidence metric ($CurrConf(R_j)$). Variable (G) represents the number of times[h] to increase or decrease confidence. G?s calculation is specific to each factor. If G is calculated to a negative value, this indicates that β should be used instead of α. Examples are shown in Section ?Confidence calculation examples?. The following sections briefly detail how each factor influences G; however the exact calculations are dependent on how parameter values are chosen, within an implementation.

$$\gamma(G,\alpha,\beta) = \begin{cases} \alpha & \text{if } G \geq 0 \\ \beta & \text{otherwise} \end{cases} \tag{5}$$

$$Conf(R_j) = (CurrConf(R_j) \quad 1)(1 \quad \gamma(G,\alpha,\beta))^G + 1 \tag{6}$$

Majority

Majority based trust is incorporated into our framework as a core algorithm for determining the trustworthiness of an agent, to then dictate whether to believe the congestion value reported about a road, which influences path planning. Section ?Background: multi-faceted trust model? describes majority based trust as a consensus, with a value which has been agreed upon by many agents. For our proposed non-Boolean extension to trust modeling, majority based trust is described as an opinion, where a similar value has been agreed upon by many agents. The rationale for the change from a Boolean based congestion value to a numerical congestion value was described in the beginning of Section ?Our proposed numeric trust modeling?.

The advice is used by choosing and prioritizing information from various reports and calculating a majority opinion, which is followed if its confidence is above a threshold, similar to the threshold of Equation 4. The primary advice presented in Section ?Background: multi-faceted trust model? would be road congestion reports, which would be used to help an agent decide what roads to take and which to avoid by considering all the facets of the multidimensional trust model. This continues to hold in our framework. In our calculation, if the confidence is below a threshold, then the advice is used from the report with the highest confidence.

The majority opinion is calculated using Algorithm 4. All relevant advice reports referencing a location are retrieved and prioritized into a list of size n. The majority opinion is then calculated, stored, and reported back to the agent. If a report contains information that is suspicious with respect to other reports that have been observed, such as an extremely high congestion report, the sender is reported as a suspicious agent. Labeling agents as suspicious is helpful in order to remove them from consideration, regardless of their current trustworthiness value. The framework will then process the suspicious agent, profiling it and updating its trust value in the knowledge base.

Algorithm 4: New Majority Computation Steps, with Numerical Congestion Metric

```
while on the road do
    Send requests and receive responses;
    if in need of advice then
        Choose $n$ reports $R$; //number of reports to use for advice
        Check Priority Road(Current Road);//to help update the Priority list
        Prioritize $n$ reports; //according to Confidence (roles, experiences, time,
        location, and if report is indirect or direct)
        foreach $n$ reports do
            if $R_j$ suspicious then
                Report suspicious agent $R_j$;
            else
                Include report $R_j$ in Majority;
            if Majority suspicious then
                Decrease Majority confidence;
        if Majority confidence > acceptable threshold && Number of reports > n
        threshold then
            Follow advice in response;
        else
            Follow advice of report with highest confidence;
    Verify reliability of reports;
    Update users? trust values;
```

Majority calculation

Algorithm 4 is a modified algorithm from Algorithm 1, which shows the calculation of a majority opinion in the framework. The algorithm uses suspicious agent detection in helping to avoid the inclusion of congestion advice which is outside a standard deviation from the current majority congestion. The majority opinion is used if there are at least n agents to use advice from and the majority confidence is above the majority threshold.

Suspicion calculation

Suspicion detection is important to include to help avoid congestion advice that greatly deviated from the current majority. Only using advice that has similar congestion reports forms our majority opinion, rather than conceiving of majority opinion as just an average congestion of the highest trusted agents (n).

If an agent is deemed suspicious, then they are reported and the agent?s advice is not used in the majority opinion calculation. However, the reverse is possible where if an agent?s advice has higher confidence than the majority and confidence greatly deviates from the majority. If this happens then the majority confidence is decreased proportionally and the agent?s advice is potentially used as the*report with highest confidence*.

Experience

Experience based trust is the most basic type of trust and is applied to every agent in our framework. As detailed in Section ?Background: multi-faceted trust model?, it is trust as a result of direct experiences with the individual agent. This is updated when the model encounters information that it can use in a judgmental nature. An example of such information would be from detecting suspicious information being reported by an agent, encountering definitive information that can be used as a comparison factor against information previously reported by an agent, or processing the opinion of a more trusted agent about the agent in question. Since experience based trust is the most basic type of trust, this forms the basis of the confidence calculation.

This facet of trust management is very simple but powerful. Section ?Simulation results? demonstrates this through *basic* simulations which only use experience and majority based trust.

Role

Experience based trust is a powerful tool for profiling agents; however, it is often challenged in scenarios with data sparsity. Data sparsity is an absence of agents with which the resident agent has had previous experience. This is often the case in the real world where it is rare to encounter a car which you have previously profiled.

Role based trust helps alleviate the issue of data sparsity by assigning roles to agents in our framework. As detailed in Section ?Background: multi-faceted trust model?, predefined roles (e.g. police patrols, traffic reporters or taxi drivers) are assigned to all agents in the system. Different roles may be associated with different levels of trust. The model uses the four different types of roles, motivated by the classification of Minhas et al: *Ordinary*, *Seniority* (e.g. commuter pool), *Expert* (e.g. news station car), *Authority* (e.g. police).

Role based trust is incorporated into a proposition?s confidence calculation by increasing it by a magnitude proportional to the particular role?s rank. Equation 7 shows how *G* is calculated for Equation 6. *RPenal* is a standard value for weighting roles, and *RoleRank* is the rank of the roles. *G* is inversely proportional to *RoleRank* so that higher roles (*Authority* has *RoleRank* of 2) warrant greater increases in confidence.

$$G = RPenal/RoleRank \tag{7}$$

Time/Location

It can often be the case that an agent receives a great deal of reports about a road, with some being more accurate than others. A combination of time and location closeness is used in confidence calculations to determine how accurate reports are. Time closeness is a measure of how old the report is with respect to when the advice is needed. Location closeness is a measure of how how far the agent providing the report is to the road in question.

Time and location closeness helps alleviate the issue of old and inaccurate reports by assigning these metrics to traffic report propositions and using them in confidence calculations in our framework. As detailed in Section ?Background: multi-faceted trust model?, metrics of time and location closeness are used in calculating a majority consensus. Our proposed model similarly uses these metrics in calculating a majority opinion, through modifying the confidence of propositions by a magnitude inversely proportional to these metrics[i].

Equations 8 and 9 show how *G* is calculated for Equation 6. *TPenal* and *LPenal* are standard values for weighting time and location respectfully. *TimeDifference* and *LocDifference* are time difference and location difference respectively. *MultiplicativeFactor* is a standard multiplicative factor for the calculation (max confidence increase will be *MultiplicativeFactor*, and not 1, if *TimeDifference* or *LocDifference* is 0.). The calculation finds the difference, for example, between *Time Difference* and *TPenal* and then divides the difference by *TPenal*. This achieves the purpose of scaling the values to be within their unit metrics[j].

$$G = (TPenal \quad TimeDifference)/TPenal * MultiplicativeFactor \tag{8}$$

$$G = (LPenal \quad LocDifference)/LPenal * MultiplicativeFactor \tag{9}$$

Direct/Indirect

The framework of this paper also incorporates the distinction of direct and indirect reports. Direct reports are reports which have been directly observed and reported by an agent. Indirect reports are direct reports of a third agent which are stored in the knowledge base of the agent the resident agent is communicating with.

For example, when one agent (Ar) communicates with another agent (A2) through a pull request concerning a priority road (R1), A2?s highest confidence traffic report concerning R1 may have been reported by another agent (A3) and not A2. A2 would send Ar the report and indicate that it is an indirect report[k] (A2 did not create the report), which would include A2?s confidence of the report. A2 calculates the confidence using the report?s experience and role based trust, and time closeness[l].

The inclusion of indirect reports, as opposed to only allowing direct reports, is important because it greatly increases the response rate of a pull request concerning a priority road. Indirect reports, however, may be more inaccurate than direct reports. This is taken into consideration through the use of the corresponding agent?s confidence of the report (A2?s confidence of the report) and by modifying the confidence value of a report by a predetermined factor.

Equation 10 shows how *G* is calculated for Equation 6. *InPenal* is a standard value for penalizing indirect reports, and *IfIndirect* is 1 if the report is indirect and 0 otherwise.

$$G = InPenal * IfIndirect \tag{10}$$

Confidence calculation examples

This subsection presents two examples which describe how the confidence metric for a report is calculated according to the multidimensional trust factors of experience and role based trust, location and time closeness, and whether the report is indirect or not. The following examples will show iterative modifications to the confidence value of a report according to the various factors.

The following calculation demonstrates how the confidence value for the report was calculated. Note that all the parameter values used in these examples are the ones used in our implementation[m].

Example 1. (illustrating α)

$$
\begin{aligned}
\text{Confidence} &= \mathit{Agent\_}39 : \mathit{trust\_degree}\ (0.6)\\
G_{time} &= (\text{TPenal}(90) \quad \text{TimeDiff}(18))/\text{TPenal}(90)\\
&\quad *\text{MultiplicativeFactor}(1.5)\\
G_{time} &= 1.2\\
\text{Confidence}(0.6) &= (\text{Confidence}(0.6) \quad 1)(1 \quad \alpha)^{|G_{time}|} + 1\\
\text{Confidence} &= 0.6475\\
G_{loc} &= (\text{LPenal}(200) \quad \text{LocDiff}(100))/\text{LPenal}(200)\\
&\quad *\text{MultiplicativeFactor}(1.5)\\
G_{loc} &= 0.75\\
\text{Confidence}(0.6475) &= (\text{Confidence}(0.6475) \quad 1)(1 \quad \alpha)^{|G_{loc}|} + 1\\
\text{Confidence} &= 0.674
\end{aligned}
$$

Example 2. (illustrating β)

$$
\begin{aligned}
\text{Confidence} &= \mathit{Agent\_}41 : \mathit{trust\_degree}\ (0.7)\\
G_{role} &= \text{RPenal}(8)/\text{RoleRank}(2)\\
G_{role} &= 4\\
\text{Confidence}(0.7) &= (\text{Confidence}(0.7) \quad 1)(1 \quad \alpha)^{|G_{role}|} + 1\\
\mathit{Confidence} &= 0.8032\\
G_{time} &= (\text{TPenal}(90) \quad \text{TimeDiff}(180))/\text{TPenal}(90)\\
&\quad *\text{MultiplicativeFactor}(1.5)\\
G_{time} &= \quad 1.5\\
\text{Confidence}(0.7813) &= (\text{Confidence}(0.7813) \quad 1)(1 \quad \beta)^{|G_{time}|} + 1\\
\text{Confidence} &= 0.7413\\
G_{loc} &= (\text{LPenal}(200) \quad \text{LocDiff}(500))/\text{LPenal}(200)\\
&\quad *\text{MultiplicativeFactor}(1.5)\\
G_{loc} &= \quad 2.25\\
\text{Confidence}(0.7604) &= (\text{Confidence}(0.7604) \quad 1)(1 \quad \beta)^{|G_{loc}|} + 1\\
\text{Confidence} &= 0.6100\\
G_{indirect} &= \text{InPenal}(\quad 2) * \text{IfIndirect}(1)\\
G_{indirect} &= \quad 2\\
\text{Confidence}(0.6991) &= (\text{Confidence}(0.6991) \quad 1)(1 \quad \beta)^{|G_{indirect}|} + 1\\
\text{Confidence} &= 0.4385
\end{aligned}
$$

Travel decisions when using numeric trust modeling

Algorithm 4 clarifies whether an agent will choose to take a certain road or not based on consensus about the congestion on the road. If the agent wants to reason about which road to choose (from a set of possible roads), it can run Algorithm 4 for each road. This algorithm is of use in scenarios such as the simulations we present in the following section, where a path planning algorithm is considering specific roads in order to propose the one that is best for the agent?s decision making. This algorithm continues to clarify our proposal for integrating trust modeling into agent decision making, in these travel environments.

Simulation results

This section describes the simulation tests performed to compare and contrast the effectiveness of our model?s implementation against a system that does not use traffic information in routing and a best case scenario. Included in the comparisons displayed in our graphs are less comprehensive trust modeling options. (For example, our proposal with only experience-based and majority-based trust modeling is one comparator; another is an algorithm that takes all reports at face value and does not incorporate trust modeling at all).

We have designed an extensive simulation testbed that can be used to validate our model by modeling traffic flow within an environment, tracking the path times of cars to determine the effectiveness of travel decisions. When vehicles make path planning decisions based on reports from other agents, if the accompanying trust modeling has been effective, the vehicles? completion of travel paths should be timely. The implementation makes use of the following third party software, JiST/SWANS, vans, DUCKS, and Protege[n]. JiST stands for Java in Simulation Time; it is a high-performance discrete event simulation engine that runs over a standard Java Virtual Machine (JVM). SWANS stands for Scalable Ad-hoc Network Simulator; it is built on top of the JiST platform and serves as a host of network simulation tools. Vans is a project comprising the geographic routing and the integrated Street Random Waypoint model (STRAW). STRAW utilizes an A* search algorithm to calculate shortest path to a destination. It also allows realworld traffic to be simulated by using real maps with vehicular nodes (briefly illustrated in Appendix D). DUCKS is a simulation execution framework, which allows for a Simulation Parameters file to be provided to define the simulation. Protege is a free, open source ontology editor and knowledge base framework. Note that the simulation constructed here, while inspired by that employed for the original model of [3], goes far beyond, to enable a rich modelling of traffic scenarios with effective measurement of successful travel.

The simulation was set to poll cars every 6?15 seconds; with 100 cars in total, experience with every other car would be gained quickly[o]. In order to simulate environments with low experience-based trust, we introduce a variable called sparsity. For example, 80% sparsity resembles having a lack of previous experience with 80% of the agents. In the simulation, this variable effectively ignores updates of trust values, thus hindering experience-based trust.

These graphs chart the performance of simulations that either use trust modeling (i.e. profiling (P), (Hon #) or not[p] (no P, Hon #)). Agent honesty represents the percent of honest agents in the simulation (i.e. 0.5 is 50% honesty). Role-based trust (Role #) represents the percent of agents in the simulation that have been assigned a role (i.e. 0.2 will have 20% of agents assigned a role). Sparsity (Spars #) represents the percent sparsity in the simulation (i.e. 0.8 will have 80% sparsity). Dishonest lie percentage (Lie #) represents the percent of the time which a dishonest agent will lie (i.e. 0.8 means dishonest agents will lie 80% of the time)(set at 100% if unspecified).

In Appendix B we display the various parameters set for the experiments and how the values were chosen (while the path planning for the simulation is displayed in Appendix C). Our first set of experiments incorporated experience-based trust and majority-based trust, alone. These were the central elements of the original model of [1-3]. We call this type of simulation Basic. Simulations with all the other additional components added are referred to as Full. The other trust modeling components individually indicated are time closeness (Time), location closeness (Loc), and indirect advice (Indir). (Full) indicates when all multidimensional trust components are being used. The VANET trust modeling results are also compared against two additional simulations: the first is a worst case scenario where traffic is ignored (no traffic)[q], and the other is a best case omnipresent version (omni) which simulates the ability for any car to look up the exact congestion of any road at anytime. All simulation tests results are averaged over 5 runs.

Figure 1 examines the average path time (appropriate due to the ultimate goal of reducing the travel time of users). This figure compares the worst case scenario against the best case scenario and various simulations which use our VANET system with the *Basic* simulation settings, at different degrees of honesty. Greater average path time in the figure indicates lower performance. The *Basic, Hon 0.1* simulation did much worse than the other *Basic* simulations most likely due to the extreme lack of trustworthy agents, but it still performed significantly better than the *Basic, No P, Hon 0.1* simulation. The *Basic* curves that incorporate trust modeling show approximately a 35% decrease in average path time over the worst case scenario. The curves in the scenarios are representative of the simulations approaching a steady state. Another observed trend is the tendency for the profiling-enabled simulations to reach a steady state faster than the other simulations. The curves here are useful for the next experiment described below.

Figure 2 compares the worst case scenario against the best case scenario and various simulations which use our VANET system with the *Full* (all trust multidimensional trust components activated) simulation settings, at different degrees of honesty. As seen in the figure, all of the simulations that used our trust modeling framework (*Full*) or the omnipresent setup averaged close to the same path time at the end of the 10000 second simulation. The other simulations produced a predictably declining performance as the

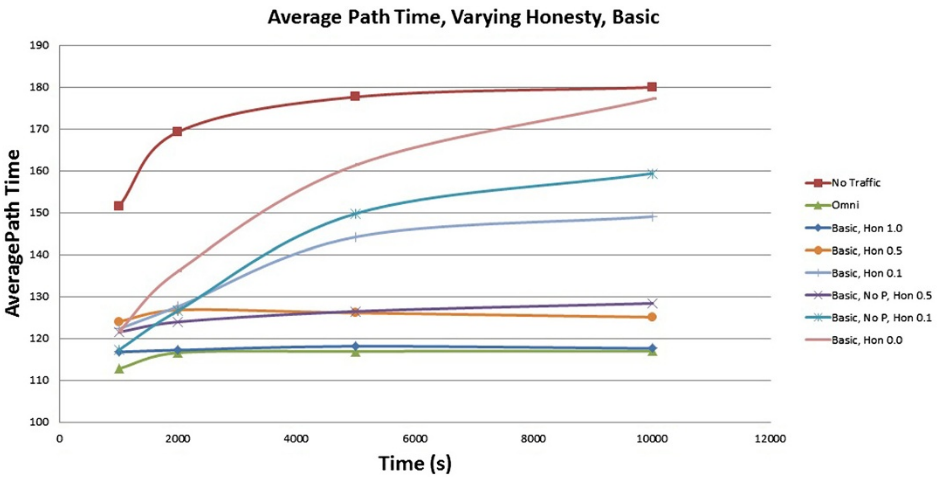

Figure 1 Avg Path Time comparison of our *Basic* model vs. best case, worst case, and *No P* scenarios.

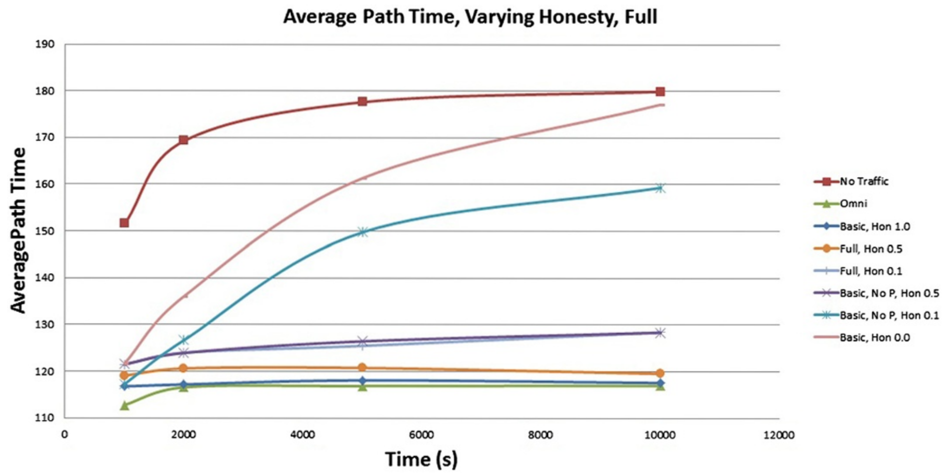

Figure 2 Avg Path Time comparison of our *Full* model vs. best case, worst case, and *No P* scenarios.

honesty percentage approached the worst case scenario. In contrast with Figure 1, *Full* simulations performed significantly better compared to the *Basic* simulations of similar honesty.

Figure 3 compares the average path time, at 10,000 seconds, of the *No Traffic*, *Omni*, *Basic*, *Basic, No P*, and *Full* scenarios, across a range of honesty values. *No Traffic* and

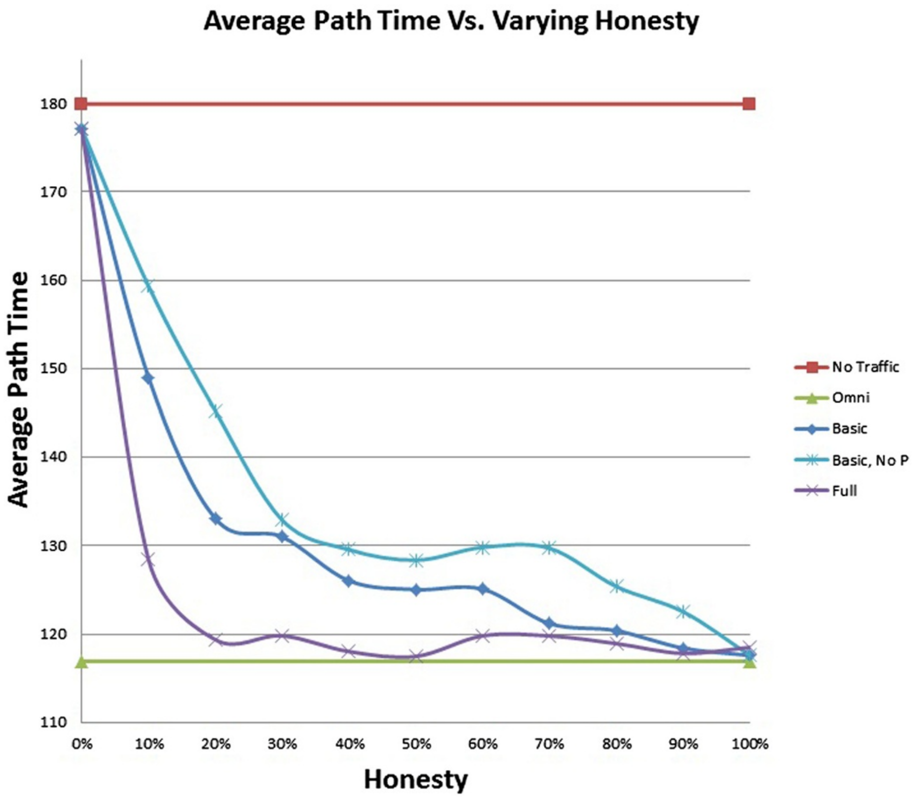

Figure 3 Avg Path Time comparison of simulation types over varying degrees of honesty at 10,000 seconds.

Omni are shown as straight lines because they do not use honesty values, but are useful as comparisons. The figure clearly shows the effectiveness of our framework across the range of honesty values. The *Basic* scenario consistently performs better than the *Basic, No P* scenario. The *Full* scenario also consistently performs better than the *Basic* scenario. All of the framework enabled simulations have a similar average path time at 0% honesty because they have no useful traffic data (and at 100% honesty because there are no untrustworthy agents to deflect through profiling). Figure 3 clearly demonstrates the impact dishonest agents can have on simulations (*Basic, No P*) and the effectiveness our proposed model framework scenarios (*Basic* and *Full*) can have on countering the influence of dishonest agents.

Figure 4 demonstrates the increased effectiveness of each of the multidimensional trust components described in Section ?Our proposed numeric trust modeling? The incremental components demonstrated are the base system (experience and majority based trust), then role based trust (Role 0.2), time and location closeness (Time, Loc), and indirect advice (Indirect). These simulations also simulate honesty at 50%, data sparsity at 50%, and additionally compare them to the best case scenario[r]. As seen in the figure, the incremental addition of trust components demonstrated predictable and substantial increases in performance. The simulation with sparsity enabled showed a predicably worse performance than its counterpart. This reflects the fact that when one has little experience-based trust, one makes poorer decisions. The simulation with role-based trust enabled shows a dramatic increase in performance, which demonstrates the impact roles have in situations with data sparsity. The best case scenario and the simulations with the higher number of trust components averaged close to the same path time at the end of the 10000 second simulation. The curves in the scenarios are representative of the simulations approaching a steady state. Another observed trend is the tendency for the component-enabled simulations to have a steadier state than the other simulations.

Figure 5 explores variations in parameter values to demonstrate the robustness of our proposed framework. We note that, even if there are very few roles assumed or if dishonest agents lie inconsistently, our framework is able to adapt and yield excellent

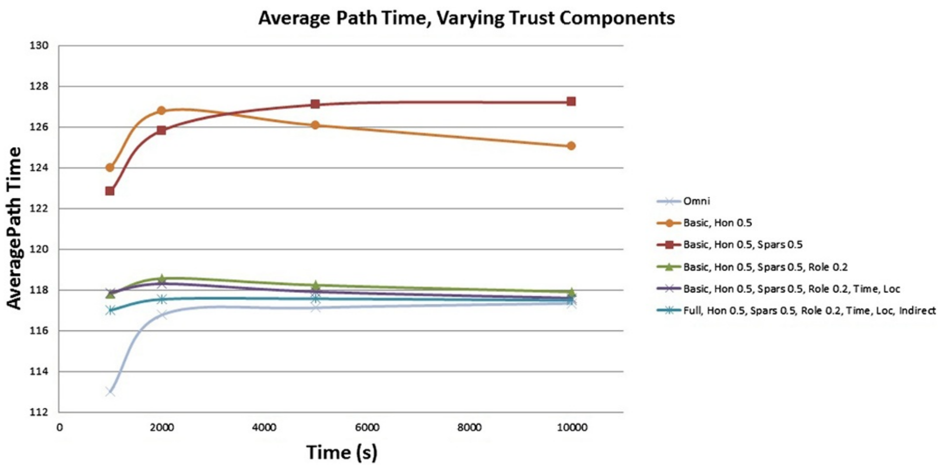

Figure 4 Avg Path Time comparison, multidimensional trust component variations.

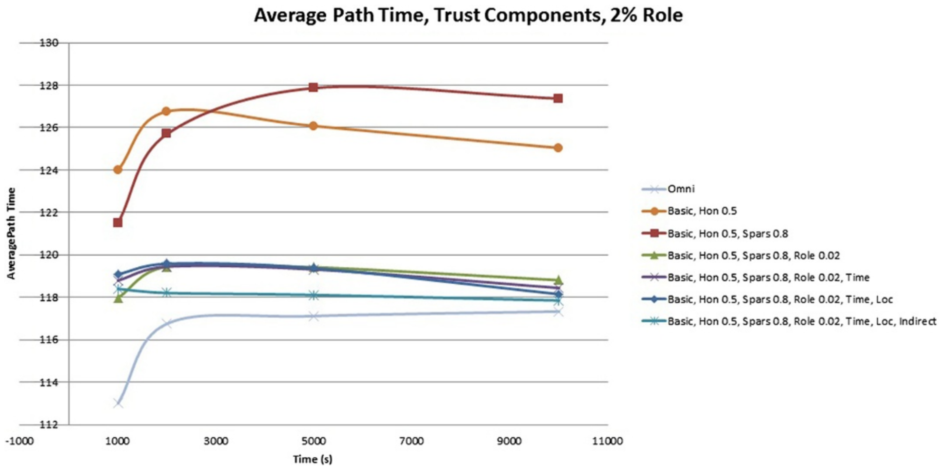

Figure 5 Avg Path Time comparison, multidimensional parameter variations.

performance, approaching that of the *Omni* (omniscient) curve. When using all dimensions (at least some or all of role, time, location, indirect), being more challenged with experienced-based trust (higher sparsity) degrades performance slightly as does having less role-based trust to rely on.

The final set of graphs show the robustness of our simulation framework through experiments that modify simulation-specific variables, such as the number of agents and messaging frequency.

Figure 6 compares the average path time, at 10,000 seconds, of the *No Traffic*, *Omni*, *Basic*, *Basic, No P*, and *Full* scenarios, across a range of values for the number of agents in the environment. The figure clearly shows the robustness of our framework across the span of agent values. The simulations around 50 agents have approximately the same path time because with such a small number of cars there is no real need for using traffic information in path planning. When increasing the number of agents, the *Basic* scenario consistently performs better than the *Basic, No P* scenario. The *Full* scenario also consistently performs better than the *Basic* scenario, when there are more than 50 agents. Figure 6 clearly demonstrates the robustness and scalability of our proposed model framework and implementation across a range of values for the number of agents in the environment.

Figure 7 compares the average path time, at 10,000 seconds, of the *No Traffic*, *Omni*, *Basic*, *Basic, No P*, and *Full* scenarios, across various messaging intervals (where x-y means that messages are sent every x to y seconds)[s]. The purpose of the figure is to demonstrate the robustness of the simulations when there are more or fewer messages. *No Traffic* and *Omni* are shown as straight lines because they do not use communication protocols, but are useful as comparisons. The figure clearly shows the robustness of our framework, especially the *Full* scenario, across various messaging intervals. The *Basic* scenario consistently performs better than the *Basic, No P* scenario until the message interval increases to (12?30 seconds) at which point the two lines are comparable. (This is because Basic is no longer receiving information at a sufficient frequency). The *Full* scenario consistently performs better than the Basic scenario, with a more gradual decrease in performance as the message interval increases[t].

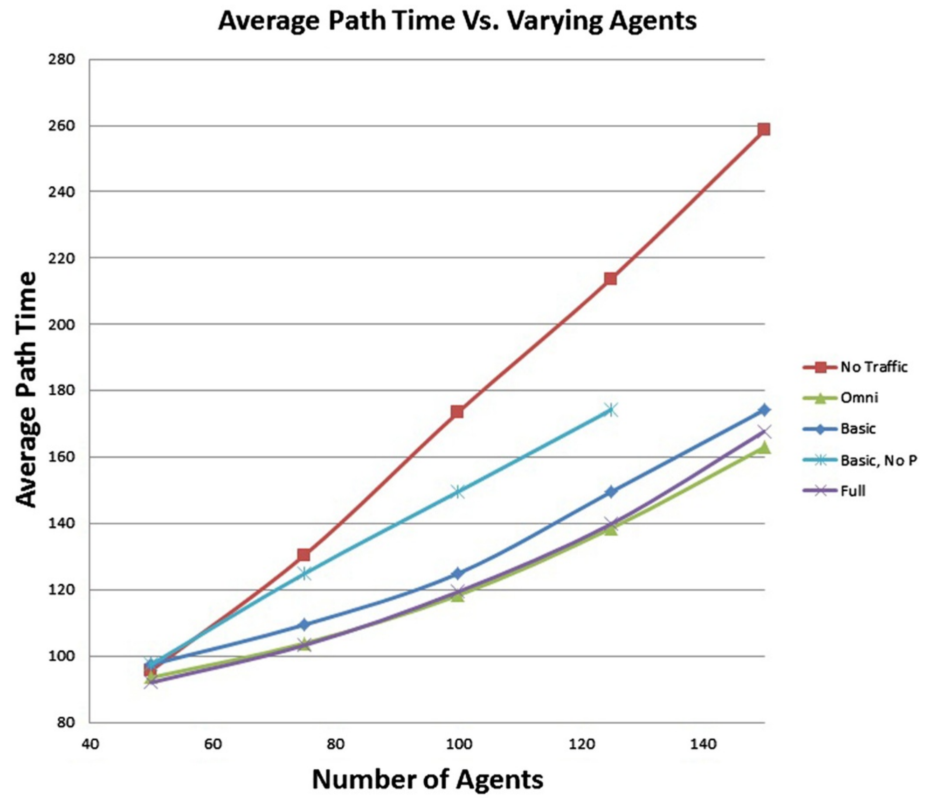

Figure 6 Avg Path Time comparison, varying number of agents.

Figure 8 compares the average path time, at 10,000 seconds, of the *No Traffic*, *Omni*, *Basic*, *Basic, No P*, and *Full* scenarios, with various communication protocols enabled. *No Traffic* and *Omni* are listed under *No Msgs* because they do not use communication protocols, but are useful as a comparison. This figure is important for backing up our claim in Section ?Agent communication protocols to exchange reports? that replacing the pull protocol, for requesting agent location and congestion data, with the push protocol, which more simply sends out the resident agent?s location and congestion data, does not impact performance. Our design rationale for this was to reduce the number of messages sent between agents.

Discussion and related work

The results presented in the previous section offer detailed experimentation incorporating a variety of metrics to validate the effectiveness of our proposed model. The experimental evidence presented serves to provide impressive confirmation of the value of the multi-faceted trust modeling algorithm that is central to the proposed decision making of the vehicles. With our particular trust modeling in place, even in scenarios where there is considerable deception in the environment, our vehicles are able to perform their path planning extremely well, maintaining an effective travel time, without significant compromise from poor path selection. This paper offers a wealth of experimental evidence to examine the proposed new trust model in considerable detail, in a thorough way. All of this is demonstrated due to our significant simulation testbed that can be used

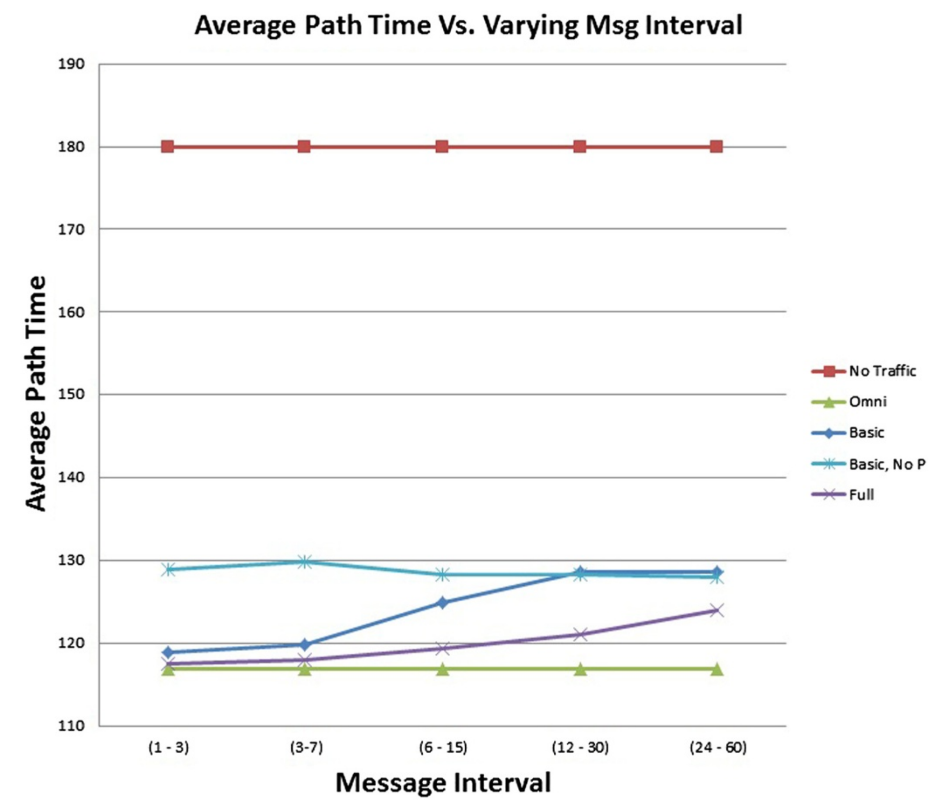

Figure 7 Avg Path Time comparison, varying message interval.

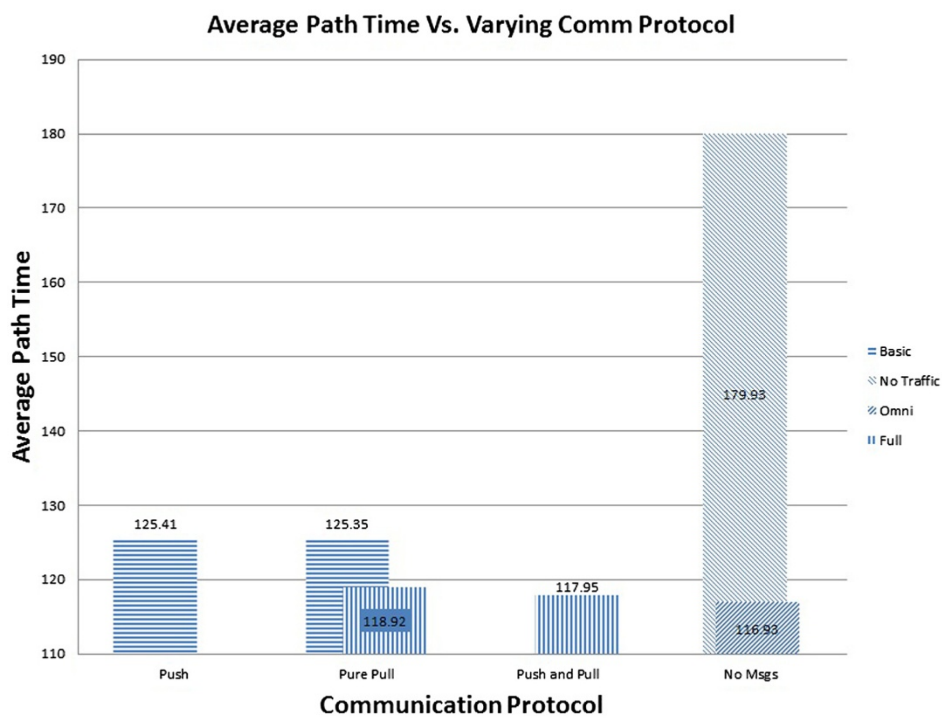

Figure 8 Avg Path Time comparison, varying number of agents.

to simulate actual traffic flow with large numbers of cars in a general mobile vehicular ad-hoc network (and as such constitutes one of the contributions of our work).

The model presented in this paper is one component of a larger framework that we designed, in order to effectively exchange and record reports between vehicles in order to direct travel decision making. In particular, we have developed more detailed proposals for employing ontological representations, for modeling users and for updating parameter values, the details of which have been omitted from this paper. It is important to note, however, that the reasoning component of our overall framework is designed to operate autonomously on a separate thread from all other implementation components. The only interaction with other components comes from other components issuing tasks to the reasoner?s queues. These tasks are either agents of interest or recently updated local road segments. These are subsequently processed and result in an update to one or more agents?t trust variables or no action at all. Agents of interest are agents that have demonstrated either a highly accurate or inaccurate report during a congestion evaluation. Recently updated local road segments are road segments and their congestion value, which have been reported directly from the resident agent. The reasoner can ultimately inspect its knowledge base to evaluate any propositions that were reported in within a specific time of this local report. Additional details are offered in [5].

We note that our simulation is to model a scenario where the actual reports are being exchanged by drivers (in cases where they may be extreme frequency, due to the number of cars on the road). While the car?s speed (as mentioned) can be reported as a stand-in for congestion, certainly GPS readings could form the basis for some automatic vehicle to vehicle reporting. We discuss the potential use of GPS as part of future work, in Section ?Conclusion and future work? Note that indirect reports are simply reports that have been forwarded by other parties and not derived from direct observation.

A focus of the research presented in this paper is our proposal for reasoning with numeric information provided by agents, set in a framework for modeling trustworthiness according to confidence values. How majority consensus can be computed for non-Boolean trust modeling is clarified in detail. This research may be of value to trust modeling researchers considering a variety of possible applications. While we have sketched our proposed formulae and their validation in the context of a specific VANET application, the approach is applicable to any scenario where experience-based trust and majority consensus are to be integrated into the overall determination of user trustworthiness. The formulae in use would simply omit the undesired elements of Equation (3): for instance, time and location may be irrelevant. The remaining calculations would remain the same.

The framework presented in this paper required a calculation of majority consensus in order to guide the decision making of a user. Other researchers have integrated majority opinion into their trust modeling but have instead used this calculation to reflect the general reputation of an agent (e.g. just how trustworthy a user is may be represented as a numeric value calculated as the average of all the scores provided by peers (say 1 for trustworthy and 0 for untrustworthy). For instance, Zhang and Cohen [6] have calculations that integrate a public reputation into the trustworthiness calculation and that also weight the contributions provided by peers according to the estimated trustworthiness of each of the advisors. The Beta Reputation System (BRS) [7] filters out advice about a user that is not in the majority and makes use of the rest of advice to model the reputation of that user. We integrate here important consideration of time and location as well, in order to value more highly the reports from users closer to the destination. In so doing, we are able to weight the combination of majority and experience based considerations more appropriately.

Others have employed a social network for trust modeling (e.g. [8,9] consider trust propagation in a network but this is less relevant in our sparsely populated environment) and others propose the use of stereotypical trust [10] (but in our domain a small set of roles can be used to reflect levels of trust.) Wang and Vassileva [11] also describe trust as multi-faceted; this work is more focused on having trust calculated differently in distinct contexts. In addition, their selection of peer advice is based on similar preferences; for our domain, location of the user and the time of its report are more critical determinants.

Some trust modeling research has introduced Dirichlet distributions in order to represent trustworthiness as something other than a pure binary value, then predicting the values of variables based on past experience. BLADE [12] models the evaluation function of advisor agents in this way, but this research is not focused on how to set decision making afterwards based on this form of trust modeling. The model of Fung et al. [13] is focused more on direct experience decision making, so not on evaluating the trustworthiness of the reports of third parties.

Our work also contrasts with other efforts currently proposed for traffic decision making[u]. Also focusing on the modeling of the trustworthiness of vehicular entities, the sociological trust model proposed by Gerlach in [14] shares some similarities with the multi-faceted trust management framework of Minhas et al. [1-3]. Gerlach has identified various forms of trust including situational, dispositional and system. Additionally, he presents an architecture for securing vehicular communication. However, he does not provide a formalization of the architecture for combining the different types of trust together. Raya et al. [15] propose data-centric trust establishment that deals with evaluating the trustworthiness of the data reported by other entities rather than trust of the entities themselves. One of the shortcomings of their work is that trust relationships in entities can never be formed; only ephemeral trust in data is established. Golle et al. [16] also present a technique that aims to address the problem of detecting and correcting malicious data in VANETs. Their approach maintains a model of every entity which contains all the knowledge that a particular entity has about the VANET. Incoming information can then be evaluated against the entity?s model of the VANET. If all the data received agrees with the model with a high probability, then the entity accepts the validity of the data. However, this approach assumes that each vehicle has global knowledge of the network and solely evaluates the validity of data, which may not be feasible in practice. Dotzer et al. [17] have suggested building a distributed reputation model that exploits a notion called opinion piggybacking where each forwarding entity (of the message regarding an event) appends its own opinion about the trustworthiness of the data. This approach 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 which generated opinions later, which may be undesirable. Patwardhan et al. [18] propose an approach in which the reputation of an entity is determined by data validation. In this approach, a few entities, 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 entities when determining the majority consensus.

Compared with the above mentioned trust modeling work, our work also provides a detailed design and implementation for the communication protocols between agents in the VANET environment, clearly specifying how an agent sends a request for location and congestion information and how an agent makes use of requested information as part of its travel decision making. This outlines how agents can effectively operate and interact with each other in order to facilitate traffic flow within their multiagent system. Another contribution offered is a proposal for reasoning with information that has been obtained through frequent broadcasting and polling. This is distinct from simply requesting information just prior to a critical decision, which may be challenging for environments such as ours with dynamic change and real-time decision requirements.

In all, the approach presented in this paper coincides well with several desiderata for designing multiagent systems for vehicular transportation, as expressed by other researchers. For example, our efforts to provide detail on the communication needed in order to support effective travel decision making also coincides well with the arguments made in [19]: that collaboration between vehicles is important and that communication is a necessary component for effectively resolving that coordination. In addition, our paper outlines how a multiagent trust model can assist in directing vehicles with travel decision making, of assistance in the managing of traffic on our roads. The importance of appropriately managing traffic has been discussed at length in [20], which outlines well the potential that techniques from artificial intelligence afford to assist in the management of this important problem. That paper in fact also points out the need for effective frameworks for simulating the network. The testbed that we develop in our research may be of some assistance in helping to resolve this challenge.

Our final reflection on related work discusses additional efforts within the current literature on developing simulations for VANET environments and research that draws out the connection of trust modeling to the messaging networks of MANETs.

At the Agents and Transportation workshop of AAMAS 2014, two papers introduced new proposals for agent-based simulation of traffic and transportation. The work of Taillander [21] is interesting in that it allows the fine tuning of various unusual traffic scenarios as part of the representation (e.g. car accidents). With this kind of focus, very large networks were also supported in the simulation. This effort does not consider messaging and trust modeling (but these may be quite interesting extensions to consider, within this context). The model developed by Huynh et al. [22] is most interested in representing the collective behaviour of drivers through various simulations, but is of interest as it focuses on addressing traffic density and on modeling drivers in the environment as decision makers. within the literature on modeling trust in VANET environments Two recent short papers offer additional suggestions for simulations in VANET environments. Chou and Lan [23] clarify that simulations are critical to properly test VANET communication models. They are interested in modeling the effects on network behaviour of traffic light changes and cars overtaking each other. Their simulations cover l000 seconds for 300 cars (in comparison to our tracking of up to 10000 seconds for examination of 100-car average path time). Piokorwski et al. [24] emphasize the importance of realistic simulations and highlight the central role of information exchange; they note that the traces of their proposed simulation can be used within the JiST/SWANS environment, to acknowledge its value as a platform. Their exploration of how to play with the mobility of various vehicles is an interesting additional feature that is offered.

MANETs compared to VANETs surfaces as a theme in the survey paper of [25]. VANETs are claimed to have greater issues of mobility of nodes and network fragmentation. The paper in turn introduces us to two papers that also provide relevant comparison to our own work, ones that are more focused on networking characteristics. Shaik and Alzaharani [26] have a concern with trust focused more on the proliferation of false identities; false location and time are both cited as of interest, which coincides well with our proposed model. The TRIP model [27] suggests the combination of direct experience and reputation (elements contained within our model as well) but assume that a history is built up for vehicles, travelling consistently on the same roads. A final paper that helps to clarify the use of trust modeling for MANET environments is that of the TARo project [28]. An anonymous routing protocol is proposed and explained in detail. This work illustrates the important companion problem of managing identities through cryptographic research.

Conclusion and future work

In conclusion, we offer an approach for supporting reasoning about agent trust with advice from peers, whose trustworthiness is then also modeled, when non-numeric reports are provided and have shown the merit of our framework in the context of the VANET application (resulting in effective travel decisions due to the modeling of trustworthiness). As such, we offer a method that supports the exchange of more detailed trustworthiness information, leading to more precise and valuable calculations. We have outlined our method for integrating various reports from peers in full detail. We have also clarified in depth how communication between peers would take place, through a combination of push and pull protocols, in order to assure effective exchange of real-time information and to extend the original model of Minhas et al. [1-3] which left as underspecified the exchange of information between agents, for effective travel decision making. Our overall solution integrates a number of novel modeling elements (priority roads, suspicious reports) which support the final algorithm that is presented. The detailed simulation framework allows for the adjustment of a wide variety of parameters which have been implemented to draw out the benefit of the full combination of our methods for trust modeling for effective transportation decisions that support exchange of traffic information. Included here is a method for simulating a dearth of experience for experience-based trust (our sparsity parameter), which can be varied in the experiments and a variable to model the extent to which agents in the environment have specific roles which may increase their trustworthiness (the role parameter). In all, with our testbed we offer an avenue for measuring the relative benefit of different trust modeling options. Parts of this research were presented at the TRUM workshop at UMAP 2012 [29].

There are a number of avenues for future work. The obvious first direction is to explore a variety of other application domains where agents may need to rely on reports from peers that offer non-binary trust values. It would be interesting, for instance, to examine the possible value of a kind of push and pull-based communication in environments such as peer recommender systems or electronic marketplaces, where rating scales mirror the kind of non-binary reports we have been discussing. Another avenue for future work would be to enhance our current solution for our chosen application of traffic reports and transportation. In earlier work, we discussed the need to distinguish second-hand reports from first-hand reports, applying penalties for incorrect reports declared to be first hand knowledge [2]. Integrating more sophisticated methods for reasoning about the trustworthiness of reports based on whether they were in fact second hand may be of value. In addition, it is quite apparent that the collective travel decision making of the entire set of vehicles on the road is an important consideration. Each agent may be advised to make its final travel decisions by reasoning about the actions likely to be taken by other agents once they have received (perhaps similar) reports. This is another topic that we are currently exploring within our research.

The work of Bazzan et al. [30] may shed some light on how to achieve this particular goal. A form of multiagent reinforcement learning may be effective in coordinating the activities of the collective of cars on the road. The work of [19] also emphasizes the value of machine learning for vehicle coordination, again suggesting this as the most promising first step for our future efforts on this topic. Regardless, the issue of system-wide coordination is one that has been argued as of significant importance for any intelligent approaches to managing traffic, as discussed in [20]. As such, this is certainly a valuable topic for future exploration.

As a final avenue for future work, it would be useful to continue to assess the value and contribution of our simulation testbed. A useful starting point would be to explore how to employ the existing testbed for other trust models that have been developed, in order to demonstrate its robustness. One class of trust models that would be appropriate to examine are ones based on Dirichlet distributions, designed to cope with multi-valued information. Extending one of these kinds of models for decision making of agents and then demonstrating its value with the testbed that we have developed would be an interesting future project. In addition, a paper that has just recently been published [31] provides an excellent survey of agent-based technology for traffic and transportation; comparing our simulation testbed and what it offers to designers against frameworks being explored by other authors, to address other vehicular challenges, would be another very informative path for future research.

As a final comment, we clarify that this research was designed with a realworld implementation in mind as the ultimate application. Reflecting on what might actually be deployed in the future, an implementation as a phone GPS add-on we feel could actually be possible. Implementing the framework in this manner would allow for easy integration into a city?s driving population. The Android operating system and platform is a viable candidate for implementation due to its use of Java as a primary language and the capability to allow applications access to a wide range of phone systems (such as the GPS). Android phones also allow multi-threading. The phones could communicate with each other through minimal Internet access. Once we migrate to the use of GPS, we move to reflecting on the value of reports exchanged mechanically, so into a territory where deliberate misinformation by drivers is less of an issue. In any case, we acknowledge that may certainly be new avenues for the future to enable vehicles to make travel decisions based on coordinated communication with other vehicles on the road.

Endnotes

[a] For now, we are assuming that reports are coming in from vehicles on the road rather than other disassociated entities. As clarified in Section ?Agent communication protocols to exchange reports?, we distinguish those vehicles reporting first hand observation from those that are passing on information acquired indirectly.

[b] For the remainder of the paper, we use the term agent to refer to the intelligent entity that is directing the actions of its vehicle. The word user refers to the driver who will ultimately be deciding where to direct the vehicle.

[c] This integrates task-based trust. For instance, an agent may set n to be fairly small, say $n \leq 10$, if she needs to make a quick driving decision, or set a larger n if she has time to process responses.

[d] For example, setting $W(B_i) = 1/2$ for the case of direct witnesses indicates that the requesting agent values direct evidence two times more than indirect evidence.

[e] Note that a reported congestion value for instance of 23 would ideally be representing the actual number of cars on the road; for our simulation, for example, the actual number of cars is known and can be reported by truthful vehicles. Agents that are not truthful will be providing inaccurate values in their reports. It may also be reasonable for cars to report their speed and for this to be a reflection of the road?s congestion.

[f] A geometric series is necessary because the calculations are capturing atomic increases in trust values but we are reasoning about non-Boolean factors that are therefore not atomic. See Appendix A for a fuller depiction of the geometric series in question.

[g] The order of application used throughout our experiments is the one we follow in this section of the paper.

[h] Note that we use the absolute value of G as the exponent in order to ensure that the number of times is a positive number.

[i] This is consistent with the placement of these factors in the denominator of Equation 3.

[j] This required scaling was not considered in sufficient detail in the model of Minhas et al. and Equation 3.

[k] The trust model described in this paper can be incorporated with a penalty mechanism such as the one presented in [2] to more severely reduce the trust value of an agent who is not a direct witness but claims to be one, resulting in the agent not being responded/helped by other agents in the system.

[l] Location closeness is not incorporated because it is dependent on the agent who is using the report.

[m] However, we use InPenal=-2 in the example here instead for a more effective illustration.

[n] Protege is used due to our knowledge-based representation for storing trust and traffic information; the details of this part of our solution have been omitted in this paper.

[o] Note that packet delivery success for the messaging is 100%. We did not simulate packet failure since this would be too similar to just reducing the volume/frequency of messages.

[p] With no profiling, no trust modeling is done and all reports received are simply assumed to be entirely trustworthy.

[q] Routing without traffic just uses a shortest path calculation.

[r] The worst case (i.e. No Traffic) is not present so that a finer granularity of the presented simulations can be shown.

[s] Messages are sent according to intervals to avoid all agents sending messages at the same time.

[t] This more gradual decrease is likely due in part to the pull protocol requesting information on roads with more immediate priority and use, generating information on roads that will be used in decision making.

[u] A more complete discussion of trust management for VANETs can be found in the recent survey paper [32].

Appendix A Confidence geometric series

This appendix seeks to further clarify and detail the geometric series equation and design rationale for calculating confidence in Section ?Confidence calculation? and to provide examples.

In Section ?Confidence calculation? we proposed Equation 6(11) for calculating the confidence of a report. Equations 1(12) and 2(13) are used as the basis for calculating the confidence of report R_j in Equation 6(11), through a modified summation of a geometric series.

$$Conf(R_j) = (CurrConf(R_j) \quad 1)(1 \quad (\alpha\ or\ \beta))^G + 1 \tag{11}$$

The following will describe why a geometric series was necessary.

Equations 12 and 13 shown below are used to modify the trust of an agent. In the framework it is necessary to attribute a trust value to each report from an agent, which we define as confidence, due to each report having possibly different attributes, such as age and if the report was observed indirectly.

$$T_A(B) \leftarrow \begin{cases} T_A(B) + \alpha(1 \quad T_A(B)) \text{ if } T_A(B) \geq 0, \\ T_A(B) + \alpha(1 + T_A(B)) \text{ if } T_A(B) < 0, \end{cases} \tag{12}$$

$$T_A(B) \leftarrow \begin{cases} T_A(B) + \beta(1 \quad T_A(B)) \text{ if } T_A(B) \geq 0, \\ T_A(B) + \beta(1 + T_A(B)) \text{ if } T_A(B) < 0, \end{cases} \tag{13}$$

A report?s confidence is initially set to the experience-based trust of the agent that provided the report. If Equations 12 and 13 were used to atomically increase a report?s confidence according to various attributes (Time, Loc, Indirect, etc.), then their influence on confidence would be disproportionate to their value and importance. A simple solution to this issue would be to weight or multiply α and β according to the attribute (Time, Loc, Indirect, etc.). However, this can result in the confidence value being above 100% or below 0%. In addition, to solve this by simply placing a bound on the confidence value (So that max is 100% and minimum is 0%) would not be faithful to the founding research.

Equations 12 and 13 implicitly bound $T_A(B)$, and have an effect of decreasing the magnitude by which trust is increased or decreased as the trust value becomes greater or smaller, respectively. Equation 11 is intended to reflect the culmination of several increases or decreases, according to 12 and 13. If you were to graph the trust value over all atomic iterations, the graph would form a Sigmoid function (?S? curve).

Equation 14 for a geometric series is shown below. Equation 15 shows the calculation at n terms in the series. This is the type of calculation we need because we need to calculate confidence after Equation 12 or 13 has been applied n times (Equivalent to G in Equation 11). Equation 15 can not be used because it does not take into consideration the result of the previous calculation, which we need to. Equation 16 describes our calculation, after Equation 12 or 13 has been applied n times, and the series which we need to represent for our calculation. Equation 16 describes the need for each term of n terms to sum the result of all previous terms. This is due to Equation 12 and 13 multiplying α and β by $T_A(B)$ (the previous trust value). The simplification of Equation 16 is equivalent to Equation 6(11).

$$a + ar + ar^2 + \ldots + ar^{n\quad 1} = a\frac{1\quad r^n}{1\quad r} \tag{14}$$

$$a_n = ar^n \tag{15}$$

$$\begin{aligned} a_n &= a_{n0} + r(1 + / \quad a_{n0}) + r(1 + / \quad a_{n1}) \\ &\quad + r(1 + / \quad a_{n2}) + \ldots + r(1 + / \quad a_{n_{n\ 1}}) \\ &= (a \quad 1)(1 \quad r)^n + 1 \end{aligned} \tag{16}$$

Defining our confidence calculation using Equation 11(6, the simplification of Equation 16) allows us to utilize Equations 12 and 13, their Sigmoid nature and implicit bounding, use of decimal numbers for $G\,(n)$ (providing a granularity that atomic changes do not allow), and a representation of the calculation in a simple format.

The following example demonstrates the modification of confidence according the time difference attribute.

Example 3. (Modification of Confidence according to Time)

$$\begin{aligned}
&Confidence_0 && = Agent\_39 : trust\_degree\ (0.6) \\
&\alpha && = 0.1 \\
&G_{time} && = (\text{TPenal}(90) \quad \text{TimeDiff}(45))/\text{TPenal}(90) \\
& && \quad *\text{MultiplicativeFactor}(4) \\
&G_{time} && = 2(\text{Increase } Confidence_0 \text{ twice}) \\
&Confidence_0 && = 0.6 \\
&Confidence_1 && = (0.6) + \alpha(1 \quad (0.6)) \\
& && = 0.64 \\
&Confidence_{2(G_{time})} && = 0.64 + \alpha(1 \quad (0.64)) \\
& && = 0.676
\end{aligned}$$

(Again using Equation 6)

$$\begin{aligned}
&Confidence_2 && = (Confidence_0 \quad 1)(1 \quad \alpha)^{|G_{time}|} + 1 \\
& && = ((0.6) \quad 1)(1 \quad \alpha)^2 + 1 \\
& && = 0.676
\end{aligned}$$

Appendix B Simulation curves and parameters

The various curves and parameters used in our simulations are summarized in full in this appendix. Table 1 displays a fuller description of the different curves that are plotted in our figures. Table 2 lists various parameters that can be adjusted in the simulations and displays the default values that we used. Table 3 indicates the variables from our framework?s formulas which are also modeled in the simulation testbed. The ability to set all the values shown in the three tables provides deeper insight into the richness of the simulation testbed that we have designed.

Appendix C Pathing

Agents within the JiST/SWANS simulation software utilize an A* search algorithm that determines the most effective path for a car to take to its destination.

Table 1 Simulation types

Name	Description	Type
No Traffic	Simulation without our framework or any incorporation of traffic data.	Worst case scenario
Omni	Simulation without our framework but incorporations traffic data by querying the road through the JiST/SWANS simulator.	Best case scenario
Basic	Simulation with just Majority and Experience based trust.	Basic scenario
Full	Simulation with all multidimensional trust components.	Full utilization scenario
Full/Basic + (Parameter(s))	Full or Basic simulation with a modification on one or more parameters.	Special case scenario.

The A* search algorithm is the driving force behind when an agent is *in need of advice*. The algorithm is called either when a new destination is set for an agent, and the agent has to find out how to most effectively reach the destination, or if an agent?s path is reassessed during their journey, so that the algorithm can incorporate more recently received traffic information.

The A* algorithm used within our framework operates as follows:

1. It is provided with the agent⊠s current location and destination.
2. It incrementally assesses potential roads, from the current location to the destination, according to a cost.
    (a) The potential road⊠s cost is calculated as its length plus congestion (triggers *in need of advice*).

Table 2 Simulation framework variables

Parameter name	Description	Representation	Default value
Honest agents	Percent of honest agents.	Hon # (0.5 is 50% honesty)	0.5
Number of agents	Number of agents and cars simulated in the tests.	Agent # (100 is 100 agents)	100
Message interval	Interval between congestion request messages sent by the agents.	MsgI #-# (6⊠15 is 6⊠15 second message intervals)	6-15
Profiling	Use of profiling.	No P indicates no use of profiling (False)	True (Basic, Full)
Role	Use of role based trust.	Role # (0.2 is 20% agents are given a role above *Ordinary*)	0(Basic) 0.2(Full)

Time closeness	Use of time closeness factor.	Time	False(Basic)
			True(Full)

Location closeness	Use of location closeness factor.	Loc	False(Basic)
			True(Full)

Indirect messages	Use of indirect messages.	Indirect	False(Basic)
			True(Full)

Information sparsity	Percent of agent trust updates ignored to simulate data sparsity.	MThresh # (0.6 means 60% of trust updates are ignored)	0
Dishonest Lie Percent	Percent of the time a dishonest agent lies.	Lie # (0.8 is 80% of the time dishonest agents lie)	1

Table 3 Simulation algorithm variables

Parameter name	Description	Representation	Default value
Majority N	Number of agents used in a majority opinion.	MajN # (10 is 10 agents used)	10
Honest trust increase α	Standard increment to an agent⊠s trust resulting from an honesty evaluation, with a maximum value of 1.0.	α # (0.1 is 10% trust increase)	0.1
Dishonest trust decrease β	Standard decrement to an agent⊠s trust resulting from an honesty evaluation, with a minimum value of 0.0.	β # (0.2 is 20% trust decrease)	0.2
Advice trust threshold	Threshold where only agents with a trust value above this percent may be considered for advice.	AThresh # (0.41 is 41% trust threshold)	0.41
Majority confidence threshold	Threshold which the majority opinion must be above in order to be considered.	MThresh # (0.51 is 51% majority threshold)	0.51
Role penalization	Standard factor for increasing confidence depending on agent role.	RPenal #	8
Time penalization	Standard comparison factor for time closeness.	TPenal #	90
Location penalization	Standard comparison factor for location closeness.	LPenal #	200
Indirect penalization	Standard factor for modifying confidence if the advice is indirect.	InPenal #	1
Congestion weight	Standard factor for weighting the congestion value when calculating a road⊠s A* cost.	CongWeight #	20

3. It returns a list of roads which forms a path to the destination that has the least cost (which theoretically takes the shortest amount of time, according to current traffic information).

The algorithm attributes a cost to every road segment. The JiST/SWANS initially calculated this cost as the length of the road segment. In our implementation, cost is calculated as the length of the road segment and its congestion. *RoadCong* is the congestion of the road, which is multiplied by a simulation specific weight *CongWeight*. The retrieval of a road?s congestion signifies an agent being*in need of advice* from Algorithm 4.

To facilitate efficient use of congestion information, and to increase the speed of the A* search algorithm, the implementation post-processes traffic information to form majority opinions so that the information can be immediately retrieved during algorithm execution. This means that majority opinions are calculated every time new information is retrieved, which is then stored in a local hash table for constant time (O(1)) retrieval by the A* algorithm.

Appendix D Pictorial depiction of grid-like maps in simulations

In this appendix, we display one example of the grid-like maps that are used in the third-party software that forms the backdrop for our simulation testbed. Figure 9 shows a snapshot of a simulation run where bold lines are extracted road segments and small rectangles represent vehicles on the streets.

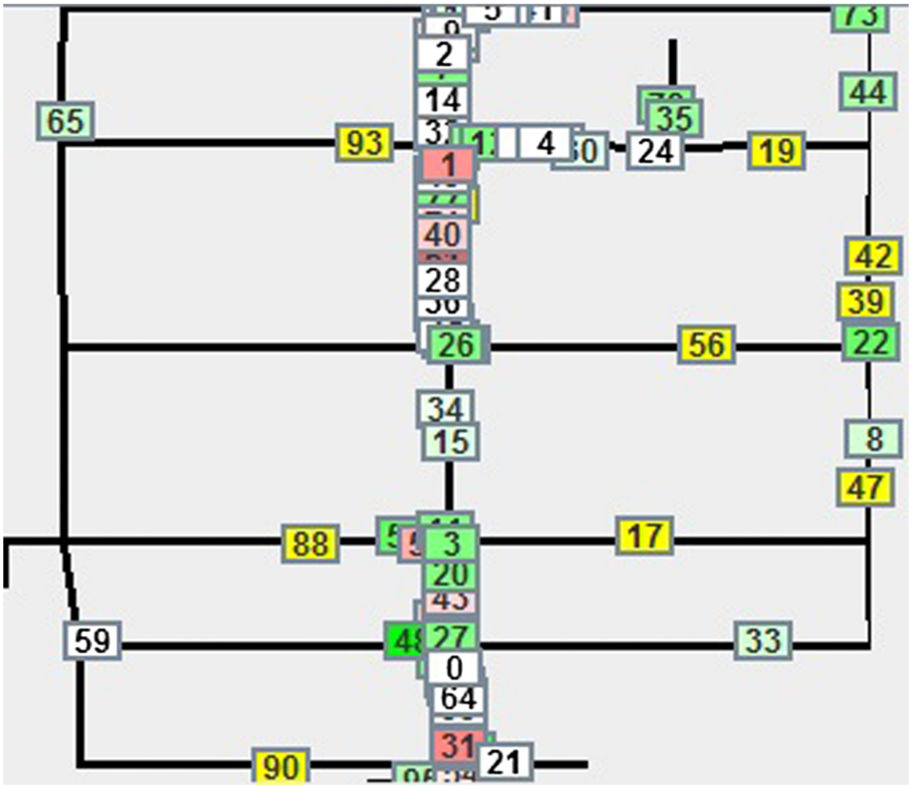

Figure 9 Simulation run of No Traffic setting.

Competing interests

The authors declare that they have no competing interests.

Authors’ contributions

JF came up with the formulation of the proposed approach and conducted experiments to evaluate the approach. RC and JZ drafted the paper. TT and UFM proofread the draft and provided comments and suggestions to improve the draft. JZ was also in charge of submitting the paper and corresponding with the editors of the journal and Springer Open Production Team. All authors read and approved the final manuscript.

Acknowledgement

Thanks to Graham Pinhey for his assistance with this paper. Financial support was received from NSERC (the Natural Sciences and Engineering Council of Canada).
Parts of this research were presented at the TRUM workshop at UMAP 2012 [29]. The work is also partially supported by the project of Dr. Jie Zhang funded by the MOE AcRF Tier 1.

Author details

[1]David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada. [2]School of Computer Engineering, Nanyang Technological University, Singapore, Singapore. [3]School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada.

Received: 24 October 2013 Accepted: 28 August 2014
Published online: 23 October 2014

References

1. Minhas UF, Zhang J, Tran T, Cohen R (2010) Promoting effective exchanges between vehicular agents in traffic through transportation-oriented trust modeling. In: Proceedings of international joint conference on Autonomous Agents and Multi Agent Systems (AAMAS) workshop on Agents in Traffic and Transportation (ATT). ACM. pp 77–86
2. Minhas UF, Zhang J, Tran TT, Cohen R (2010) 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). pp 243–247
3. Minhas UF, Zhang J, Tran TT, Cohen R (2011) A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. IEEE Trans Syst Man Cybern C Appl Rev 41(3):407–420

4. Tran T, Cohen R (2003) Modelling reputation in agent-based marketplaces to improve the performance of buying agents. In: Proceedings of the ninth international conference on User Modelling (UM). Springer. pp 273⊠282
5. Finnson J (2012) Modeling trust in multiagent mobile vehicular ad-hoc networks through enhanced knowledge exchange for effective travel decision making. Master⊠s thesis, School of Computer Science, University of Waterloo. Waterloo, Canada
6. Zhang J, Cohen R (2008) Evaluating the trustworthiness of advice about seller agents in e-marketplaces: a personalized approach. Electron Commerce Res Appl 7(3):330⊠340
7. Whitby A, J⊠sang A, Indulska J (2004) Filtering out unfair ratings in bayesian reputation systems. In: Proceedings of the Workshop on Trust in Agent Societies, at the Autonomous Agents and Multi-Agent Systems Conference (AAMAS2004), New York. July 2004
8. Yu B, Singh MP (2003) Detecting deception in reputation management. In: Proceedings of the second international joint conference on Autonomous Agents and Multiagent Systems. AAMAS ⊠03. ACM, New York. pp 73⊠80
9. Yolum P, Singh MP (2005) Engineering self-organizing referral networks for trustworthy service selection. IEEE Trans Syst Man Cybern Syst Hum 35(3):396⊠407
10. Burnett C, Norman T, Sycara K (2011) Sources of stereotypical trust in multi-agent systems. In: Proceedings of the 14th international workshop on trust in agent societies. p 25
11. Wang Y, Vassileva J (2003) Bayesian network-based trust model. In: Proceedings of the IEEE/WIC international conference on Web Intelligence (WI). pp 372⊠378
12. Regan K, Poupart P, Cohen R (2006) Bayesian reputation modeling in e-marketplaces sensitive to subjectivity, deception and change. In: AAAI. pp 1206⊠1212
13. Fung CJ, Zhang J, Aib I, Boutaba R (2011) Dirichlet-based trust management for effective collaborative intrusion detection networks. IEEE Trans Netw Serv Manag 8(2):79⊠91
14. Gerlach M (2007) Trust for vehicular applications. In: Proceedings of the international symposium on autonomous decentralized systems. IEEE. pp 295⊠304
15. Raya M, Papadimitratos P, Gligor VD, Hubaux J-P (2008) On data-centric trust establishment in ephemeral ad hoc networks. In: Proceedings of the 27th Annual IEEE International Conference on Computer Communications (IEEE INFOCOM). pp 1238⊠1246
16. Golle P, Greene D, Staddon J (2004) Detecting and correcting malicious data in vanets. In: Proceedings of the 1st ACM international workshop on vehicular ad hoc networks. ACM. pp 29⊠37
17. 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 453⊠456
18. Patwardhan A, Joshi A, Finin T, Yesha Y (2006) A data intensive reputation management scheme for vehicular ad hoc networks. In: Proceedings of the Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services. IEEE. pp 1⊠8
19. Desjardins C, Laum⊠nier J, Chaib-draa B (2009) Learning agents for collaborative driving. In: Bazzan A, Kl⊠gl F (eds). Multiagent systems for traffic and transportation engineering. IGI Global, Hershey. pp 240⊠260
20. Bazzan AL (2007) Traffic as a complex system: Four challenges for computer science and engineering. In: Proceedings of the XXXIV SEMISH. Citeseer. pp 2128⊠2142
21. Taillandier P (2014) Traffic simulation with the gama platform. In: Klugel F, Bazzan A, Ossowoski S, Chaib-Draa B (eds). Proceedings of the international conference on Autonomous Agents and Multiagent Systems (AAMAS) sixth workshop on Agents in Traffic and Transportation (ATT). pp 77⊠86
22. Huynh N, Cao VL, Wickramasuriya R, Berryman M, Perez P, Barthelemy J (2014) An agent based model for the simulation of road traffic and transport demand in a Sydney metropolitan area. In: Klugel F, Bazzan A, Ossowoski S, Chaib-Draa B (eds). Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS) sixth workshop on Agents in Traffic and Transportation (ATT)
23. Chou C-M, Lan K-c (2009) On the effects of detailed mobility models in vehicular network simulations. In: Proceedings of the ACM MobiCom
24. Piorkowski M, Raya M, Lugo AL, Papadimitratos P, Grossglauser M, Hubaux J-P (2008) TraNS: realistic joint traffic and network simulator for VANETs. ACM SIGMOBILE mobile computing and communications review 12(1):31⊠33
25. Vidhya S, Mugunthan SR (2014) Trust modeling scheme using cluster aggregation of messages for vehicular ad hoc networks. IOSR J Comput Eng 16(2):16⊠21
26. Shaihk R, Alzahrani A (2013) Intrusion-aware trust model for vehicular ad hoc networks. Security and Communication Networks. doi:10.1002/sec.862
27. Marmola FG, Pere GM (2012) Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. J Netw Comput Appl 35(3):934⊠941
28. Chen J, Boreli R, Sivaraman V (2010) Taro: Trusted anonymous routing for manets. In: Proceedings of the IEEE/IFIP 8th international conference on embedded and ubiquitous computing. pp 756⊠762
29. Finnson J, Cohen R, Zhang J, Tran T, Minhas UF (2012) Reasoning about user trustworthiness with non-binary advice from peers. Adaptation and Personalization (UMAP) workshop on Trust, Reputation and User Modeling (TRUM). pp 12
30. Bazzan ALC, de Oliveira D, da Silva BC (2010) Learning in groups of traffic signals. Eng Appl Artif Intell 23(4):560⊠568
31. Bazzan A, Klugl F (2013) A review on agent-based technology for traffic and transportation. Knowl Eng Rev:1⊠29. doi:10.1017/S0269888913000118
32. Zhang J (2011) A survey on trust management for vanets. In: Proceedings of the 25th international conference on Advanced Information Networking and Applications (AINA). IEEE. pp 105⊠112

doi:10.1186/s40493-014-0010-0
Cite this article as: Cohen *et al.*: **A trust-based framework for vehicular travel with non-binary reports and its validation via an extensive simulation testbed.** *Journal of Trust Management* 2014 **1**:10.