A Proof-theoretic Trust and Reputation Model for VANET

Giuseppe Primiero, Franco Raimondi, Taolue Chen and Rajagopal Nagarajan
Department of Computer Science,
Middlesex University London, United Kingdom
Email: G.Primiero—F.Raimondi—T.Chen—R.Nagarajan@mdx.ac.uk

***Abstract*—Vehicular Ad Hoc Networks (VANETs) are an important component of intelligent transportation systems, which are set to become part of global transportation infrastructure in the near future. In the context of such networks, security requirements need to rely on a combination of reputation of communicating agents and trust relations over the messaging framework. This is crucial in order to maintain dynamic and safe behaviour under all circumstances. Formal correctness, resolution of contradictions and proven safety of transitive operations in the presence of reputation and trust within the infrastructure remain mostly unexplored issues. This could lead to potentially disastrous situations, putting lives at risk. In this paper we provide a proof-theoretic interpretation of a reputation and trust model for VANET. This allows for formal verification through translation into the Coq proof assistant, and can guarantee consistency of messaging protocols and security of transitive transmissions.**

1. Introduction

Vehicular Ad Hoc Networks (VANETs) consist of vehicles and roadside unit networks created to enhance transportation systems through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. VANET services include: vehicle and road safety services, which target characteristics like the decrease of traffic accidents and loss of life to vehicle occupants; traffic efficiency and management services, which aim to improve traffic flow, traffic coordination, and to provide local and map information; information and entertainment services, to provide multimedia data transfer and global Internet access, [7].

Due to their distributed and dynamic nature, such networks are open to several types of threats, including false message propagation. Trust and reputation are among the most used concepts to ensure integrity, reliability and safety of services. Several methods have been implemented in VANETs to manage trust, see [14] for a recent overview. Trust models in VANETs differ in accordance to the main object of the model: entity-centric [9], [4], data-centric [12], [8] and combined [16]. The work in [15] offers an analysis that accounts for reputation as a characteristic of message forwarding among vehicles, drivers and other agents: reputation of these agents is based on a descriptive ontology and is used to provide feedback in the system. An overview of the issues related to trust in fixed and mobile ad hoc networks is given in [17], while other approaches for trustworthiness and reputation in ad hoc mobile networks are presented, for example, in [3], [2].

In most of these models, the analysis relies on simulations. However, such simulations cannot guarantee the absence of unpredictable and unsafe behaviours. Since VANETs are meant to include safety and emergency messages, more reliable methods are essential. The only method to produce exhaustive safety control is through formal verification, but unfortunately none of the current trust and reputation models seem to have focused on a formal correctness requirement to ensure that the protocols are verifiable. Formal approaches to VANET include the work in [6] for the verification of a congestion control protocol using the model checker PRISM to investigate its correctness and effectiveness; verification of privacy and authentication using the AVISPA tool in [1]; verification of the TESLA authentication protocol [5] using Petri nets. Such approaches are few and far apart. Moreover, they do not focus explicitly on trust or reputation and they are all based on model checking. Other formal verification techniques like theorem proving seem to have been ignored so far. Moreover, an additional problem, i.e., ensuring that safety is preserved over transitive operations, remains unexplored. In particular, the problem of a message passing over from vehicle v_i to v_j and from v_j to v_k illustrate the need to guarantee that for each such transition security and safety properties are preserved.

The present paper addresses both problems mentioned above. In Section 2, we formulate a proof-theoretic translation of the trust and reputation model for VANET given in [15] with an extension of the natural deduction calculus `(un)SecureND` from [10]. The aim is, first of all, to show that the trust properties instantiated through our calculus faithfully reflect those in a VANET network; accordingly, non-trustworthy interactions can be identified through a proof-checking method. On a higher level, the model offered by `(un)SecureND` has been proven formally correct through its translation to a Coq library. As such, the present translation guarantees a similar property for the whole VANET model. Thanks to the structural properties of our calculus, we show how transitive message passing operations, in the form of instances of a cut rule, are guaranteed safe via applying a normalisation result. In other words, we are able to qualify as safe a message passing operation through any number of vehicles by checking at each interaction that consistency is preserved. In Section 3, we illustrate protocols for handshaking, recipient selection and message passing based on reputation. In Section 4, we give a reputation model based on an evaluation of parametrised feedback messages, in view of a temporal measure and a ranking of the relevant service characteristic of each message.

2. (un)SecureND

Recall that (un)SecureND is a natural deduction calculus defining trust, mistrust and distrust protocols introduced in [11] and extended in [10] with a negation connective. Here we provide a slightly modified version, adapted for a VANET network. In particular, in the present version we introduce: *contexts* as sets of sets; *formulas* with multiple indices to account for service and message numbers; *ranking* on service characteristics. We start with introducing the language of the logic:

Definition 1 (Syntax of (un)SecureND).

$$\begin{aligned}
&\mathcal{A}^{\prec} := \{\mathcal{V}, \mathcal{R}\}\\
&\mathcal{V} := \{v_1 \prec \cdots \prec v_n\}\\
&\mathcal{R} := \{rsu_1 \prec \cdots \prec rsu_m\}\\
&\mathcal{S} := \{S_1, \ldots, S_n\}\\
&\mathcal{C} := \{C^{S_1}_{\vec{n}}, \ldots, C^{S_n}_{\vec{n}}\}\\
&\phi^{\mathcal{A}}_{C^{S_i}_j} := a^{\mathcal{A}}_{C^{S_i}_j} \mid \neg\phi^{\mathcal{A}}_{i,j} \mid \phi^{\mathcal{A}}_{i,j} \to \phi^{\mathcal{A}}_{k,l} \mid \phi^{\mathcal{A}}_{i,j} \wedge \phi^{\mathcal{A}}_{k,l}\\
&\qquad \mid \phi^{\mathcal{A}}_{i,j} \vee \phi^{\mathcal{A}}_{k,l} \mid \bot \mid Read(\phi^{\mathcal{A}}_{C^{S_i}_j}) \mid\\
&\qquad Write(\phi^{\mathcal{A}}_{C^{S_i}_j}) \mid Trust(\phi^{\mathcal{A}}_{C^{S_i}_j})\\
&\Gamma^{\mathcal{A}} := \phi^{\mathcal{A}}_{i,j} \mid \phi^{\mathcal{A}}_{i,j} < \phi^{\mathcal{A}}_{k,l} \mid \Gamma^{\mathcal{A}}; \phi^{\mathcal{A}}_{i,j}
\end{aligned}$$

$\mathcal{A}$ is the set of agents issuing messages containing vehicles $\mathcal{V}$ and roadside units (RSUs) $\mathcal{R}$. Below we will focus in particular on V2V communication, without loss of generality. The order $\prec$ between agents is a reputation order, defined below in Section 4. $\mathcal{S}$ denotes a set of services. $\mathcal{C}$ denotes a set of service characteristics, with each element $C^{S_i}_{\vec{n}}$ denoting the set of n characteristics of service S_i. We assume, here and throughout, that characteristics $C^{S_i}_{\vec{n}}$ of services for each service S_i are associated with an order $\leq$, so are given as *posets*, and the ordering $\leq$ is used to order messages below in Definition 4. Note that for two characteristics $C^{S_i}_{\vec{n}}$ and $C^{S_j}_{\vec{n}}$ respectively with $i \neq j$, there is no order between them.

Messages are boolean formulae, closed under connectives and including $\bot$ to express conflicts. Messages are signed by agents generating them and by service and characteristic identifiers: $\phi^{v_i}_{C^{S_k}_j}$ expresses a message ϕ about characteristic C_j of service S_k generated by vehicle v_i. To simplify, we often abbreviate this notation as $\phi^{v_i}_{k,j}$. When required, we will refer to a *set of messages* about service S_k and characteristic C_j from vehicle v_i as $\mathcal{M}^{v_i}_{S_k,C_j}$; this notation can be further generalised to a whole set of vehicles $\{v_i, \ldots, v_k\} \subseteq \mathcal{A}$. A profile for vehicle v_i, denoted as Γ^{v_i} is the current list of all messages collected by v_i from available sensors, other agents and networks. For the present purposes, information from networks will be indexed at their first receiving vehicle, so as not to add networks as separate agents. For example, a vehicle profile Γ^{v_i} receives a message $\phi_{j,k}$ about service $S_j =$ `weather` and characteristic $C_k =$ `temperature` stating $\phi = (temp \geq 5°C)$. We can now define the notion of judgement in the language:

Definition 2 (Judgements). *A judgement $\Gamma^{v_l} \vdash_{\mathtt{s}} \phi^{v_j}_{i,k}$ states that a message ϕ about service i and characteristic k signed from agent v_j is validly accessed at step $\mathtt{s} \geq 0$ under the profile of agent v_l.*

Definition 3 (Validity). *A judgement $\vdash_{\mathtt{s}} \phi^{v_j}_{i,k}$ says that a message ϕ about service i and characteristic k signed from vehicle v_j holds for any vehicle's profile at step $\mathtt{s}$.*

Messages satisfy a ranking based on characteristics:

Definition 4. *We define an order $<$ between messages such that $\phi^{v_j}_{i,k} < \phi^{v_j}_{i,l}$ holds if $C^{S_i}_k \leq C^{S_i}_l$ for a vehicle v_j.*

Therefore the order relation $\leq$ between service characteristics induces validity under profile: if a characteristic k is essential to another characteristic l with respect to a service i for a vehicle v_j, then v_j will be required to obtain a value for k in order to validly access a value for l. An example of such order between characteristics could be as follows: under the service `weather`, $C_k =$ `humidity` and $C_l =$ `precipitation − forecast`, where the former characteristic is essential to determine the latter.

A valid vehicle profile meets all the requirements and conflicts clauses of all service messages that the vehicle receives. A conflict is generated by two contradictory messages, and the profile is valid when such conflicts are avoided; a requirement is the need of a given value for some service and requirement, and a valid profile contains all such required values. We use $profile$ as a typing term to denote a sets of formulas valid for a vehicle. Profile construction by service messages requirements is defined by rules from Figure 1. We start by declaring an empty profile to be valid (base case); by Message Insertion, a valid message can be inserted in a vehicle profile; by Requirement Insertion, a profile can be extended by satisfied service requirements; by Profile Extension, if a message holds in an empty profile, it can be added to an existing profile. In this syntax, the construction of two vehicle profiles $\Gamma^{v_i}; \Gamma^{v_j} : profile$ will typically denote the existence of an active communication channel between vehicles v_i, v_j.

2.1. Rules for message construction

The operational rules in Figure 2 formulate compositionality of messages. The rule $Atom$ establishes that a vehicle and a communication channel between vehicles can qualify a message as valid if all its requirements are satisfied. Rule $\bot$ expresses that contradictory messages imply access to their negation. Rule $\wedge$-I allows to compose message originating from different vehicles; by rule $\wedge$-E, decomposition is valid for the channel obtained by the vehicles

$$\frac{}{\{\} : profile}\text{ Empty Profile} \qquad \frac{\vdash \phi_{i,k}^{v_j}}{\phi_{i,k}^{v_j} : profile}\text{ Message Insertion}$$

$$\frac{\Gamma^{v_j}, \phi_{i,k}^{v_j} : profile \qquad \Gamma^{v_j}, \phi_{i,k}^{v_j} \vdash_{\mathtt{s}} \psi_{i,l}^{v_k}}{\Gamma^{v_j}, \phi_{i,k}^{v_j} < \psi_{i,l}^{v_k} : profile}\text{ Requirement Insertion}$$

$$\frac{\Gamma^{v_i} : profile \qquad \vdash_{\mathtt{s}} \psi_{j,l}^{v_k}}{\Gamma^{v_i}; \psi_{j,l}^{v_k} : profile}\text{ Profile Extension}$$

Figure 1. The System (un)SecureND: Profile Construction Rules

from which the messages originate. Rule $\vee$-I says that a channel of two vehicles profiles can access any message produced from each of the composing vehicle profiles; by the elimination rule $\vee$-E, each message consistently inferred by each individual vehicle profile can also be executed under the channel between the profiles of the two vehicles. Rule $\rightarrow$-Introduction expresses inference of a message from a channel as inference between messages (Deduction Theorem); its elimination through rule $\rightarrow$-E allows to recover such inference as profile extension (Modus Ponens).

2.2. Access Rules

In Figure 3 we present the access rules on messages. These allow a vehicle to act on messages received from another vehicle. Rule $\neg$-distribution expresses profile consistency: if a vehicle profile does not allow inferring a message $\phi_{i,j}$, then it allows inferring any other message whose requirements do not include $\phi_{i,j}$. Rule $read$ says that from any consistent vehicle profile a message can be read provided its requirements are satisfied (if any). Rule $trust$ works as an elimination rule for $read$: it says that if a message is received by a vehicle and it preserves its profile consistency, then it can be trusted. Rule $write$ works as an elimination rule for $trust$: it says that a message readable and trustable by a vehicle can be broadcast. Rule *exec* says that every message consistently received by a vehicle is valid in it. The rule MTrust-I says that currently held message conflicting with a newly arrived message is mistrusted, i.e., removed from the current vehicle profile until none of its consequences are included; the corresponding MTrust-E elimination allows to trust any message consistent with the conflict resolution by removal of the mistrusted message in the vehicle profile, including any required dependency: this is expressed by the side condition that requires checking with any other vehicle with higher reputation than the sender of the original message. The side condition can be modified at will, e.g., to design a protocol that will restore previous information if a sufficient number of other vehicles with higher reputation support it. *mistrust* is a flag for facilitating removal of messages present in the vehicle profile conflicting in view of incoming new information.

2.3. Structural Rules

Structural rules hold with restrictions for (un)SecureND, see Figure 4. As a result, the system qualifies as substructural, see for instance [13]. Weakening is constrained by an instance of $trust$: it says that valid information is preserved under a vehicle's profile extension, assuming the latter is provably consistent. Contraction is constrained by preservation of ordering: it says that removing identical messages from a vehicle's profile is admissible, with the constraint that the copy from the vehicle with higher reputation is preserved. Exchange is constrained by dependency: it says that reorder of messages is admissible if there is no involved dependency between them. Finally, the Cut rule expresses validity under a vehicle's profile extension: if a message $\phi_{i,j}$ is valid for vehicle v_i and after messaging it to v_j the latter can infer $\phi_{i,k}$, then v_i can infer $\phi_{i,k}$ by setting a message protocol with v_j.

Theorem 1 (Normalisation)**.** *Any message $\phi_{i,k}$ valid for a channel v_i, v_j and obtained by an occurrence c of the Cut rule can be validated without c using only trust.*

Proof. By induction on the derivation D which is the redex of the cut-elimination. Assuming c is the only Cut rule and it is the last inference rule of the redex, the derivation D' which is the contractum of the cut-elimination contains a descendent of the cut obtained by an instance of Weakening under trust. Because the formula obtained by the cut is, by hypothesis, derivable from the weaker protocol, it will also be derivable from the weaker and the stronger protocol together. When c is not the last inference rule of the redex, then the descendent of the cut will admit all similar Weakening preserving the one occurring in the cut; those imports by Weakening will occur also in the contractum of the cut rule and can be traced back up to the one formulation of the import that occurs in the cut rule. $\square$

Normalisation justifies a safety property of our trust and reputation model over transitive transmissions: for each vehicle v_i, v_j, v_k, if v_k holds information $\phi_{i,j}$ and this information is passed to v_j, then every valid message derived from $\phi_{i,j}$ by v_k can be inferred by v_j assuming the consistency (by trust) of its profile with that of v_k; similarly now, v_j can pass $\phi_{i,j}$ to v_i, and the latter can infer from there, assuming its profile is consistent with those of v_j, v_k.

$$\frac{\Gamma^{v_i};\Gamma^{v_j} : \mathit{profile}}{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{s}} \phi^{v_j}_{i,l}}\text{ Atom, for any } \phi^{v_j}_{i,l} \in \Gamma^{v_j} \qquad \frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \phi^{v_i}_{i,j} \rightarrow \bot}{\Gamma^{v_i} \vdash_{\mathtt{s+1}} \neg\phi^{v_i}_{i,j}}\ \bot$$

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \phi^{v_i}_{i,l} \qquad \Gamma^{v_j} \vdash_{\mathtt{s'}} \psi^{v_j}_{i,m}}{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{max(s,s')+1}} \phi^{v_i}_{i,l} \wedge \psi^{v_j}_{i,m}}\ \wedge\text{-I} \qquad \frac{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{s}} \phi^{v_i}_{i,l} \wedge \psi^{v_j}_{i,m}}{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{s+1}} \phi/\psi^{v_{i/j}}_{i,l/m}}\ \wedge\text{-E}$$

$$\frac{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{s}} \phi^{v_{i/j}}_{i,l}}{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{s+1}} \phi^{v_{i/j}}_{i,l} \vee \psi^{v_{i/j}}_{i,m}}\ \vee\text{-I} \qquad \frac{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{s}} \phi^{v_{i/j}}_{i,l} \vee \psi^{v_{i/j}}_{i,m} \qquad \phi/\psi^{v_{i/j}}_{i,l/m} \vdash_{\mathtt{s'}} \xi^{v_{i/j}}_{k,n}}{\Gamma^{v_i};\Gamma^{v_j} \vdash_{\mathtt{max(s,s')+1}} \xi^{v_{i/j}}_{k,n}}\ \vee\text{-E}$$

$$\frac{\Gamma^{v_i};\phi^{v_i}_{i,l} \vdash_{\mathtt{s}} \psi^{v_j}_{i,m}}{\Gamma^{v_i} \vdash_{\mathtt{s+1}} \phi^{v_i}_{i,l} \rightarrow \psi^{v_j}_{i,m}}\ \rightarrow\text{-I} \qquad \frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \phi^{v_i}_{i,l} \rightarrow \psi^{v_j}_{i,m} \qquad \Gamma^{v_i} \vdash_{\mathtt{s'}} \phi^{v_i}_{i,l}}{\Gamma^{v_i};\phi^{v_i}_{i,l} \vdash_{\mathtt{max(s,s')+1}} \psi^{v_j}_{i,m}}\ \rightarrow\text{-E}$$

Figure 2. The System `(un)SecureND`: Operational Rules

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \neg\mathcal{O}(\psi^{v_j}_{i,l})}{\Gamma^{v_i} \vdash_{\mathtt{s+1}} \mathcal{O}(\neg\psi^{v_j}_{i,l})}\ \mathcal{O} \in \{\mathit{Read}, \mathit{Trust}, \mathit{Write}\}, \neg\text{-distribution} \qquad \frac{}{\Gamma^{v_i} \vdash_{\mathtt{s}} \mathit{Read}(\psi^{v_j}_{i,l})}\ \mathit{read}$$

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \mathit{Read}(\psi^{v_j}_{i,l}) \qquad \Gamma^{v_i};\psi^{v_j}_{i,l} : \mathit{profile}}{\Gamma^{v_i} \vdash_{\mathtt{s+1}} \mathit{Trust}(\psi^{v_j}_{i,l})}\ \mathit{trust}$$

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \mathit{Read}(\psi^{v_j}_{i,l}) \qquad \Gamma^{v_i} \vdash_{\mathtt{s'}} \mathit{Trust}(\psi^{v_j}_{i,l})}{\Gamma^{v_i} \vdash_{\mathtt{s'+1}} \mathit{Write}(\psi^{v_j}_{i,l})}\ \mathit{write} \qquad \frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \mathit{Write}(\psi^{v_j}_{i,l})}{\Gamma^{v_i} \vdash_{\mathtt{s+1}} \psi^{v_j}_{i,l}}\ \mathit{exec}$$

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \mathit{Read}(\psi^{v_j}_{i,l}) \rightarrow \bot \qquad \Gamma^{v_i} \setminus \{\neg\psi^{v_i}_{i,l}\} : \mathit{profile}}{\Gamma^{v_i} \setminus \{\neg\psi^{v_i}_{i,l}\} \vdash_{\mathtt{s+1}} \neg\mathit{Trust}(\neg\psi^{v_i}_{i,l})}\ \text{MTrust-I}$$

$$\frac{\Gamma^{v_i} \setminus \{\neg\psi^{v_i}_{i,l}\} \vdash_{\mathtt{s}} \neg\mathit{Trust}(\neg\psi^{v_i}_{i,l}) \qquad \Gamma^{v_k};\psi^{v_j}_{i,j} : \mathit{profile}}{\Gamma^{v_i} \setminus \{\neg\psi^{v_i}_{i,l}\};\Gamma^{v_k} \vdash_{\mathtt{s+1}} \mathit{Trust}(\psi^{v_j}_{i,l})}\ \text{MTrust-E}, \forall v_k \prec v_j$$

Figure 3. The System `(un)SecureND`: Access Rules

3. Opportunistic Forwarding

In this section we present the algorithm and exemplify derivations for handshaking and opportunistic message forwarding protocols. The algorithm consists of two parts: it first selects a recipient for the communication according to a reputation model; then it implements message forwarding if consistency is guaranteed by trust. The pseudo-code of the full protocol with handshaking and opportunistic forwarding is formulated in Figure 5. Here we use protocol operations named after the relevant `SecureND` rules, as well as symbols for vehicles, services and characteristics.

In Figure 6 we present the `SecureND` translation of the handshaking protocol. Here Service 1 identifies the set of messages for this protocol. By Hello Message, a user v_i with a well-defined profile with a 'hello' message in its recognition service sends the message to the network; a user v_k reading the message and assuming it preserves consistency (e.g. there is no instruction in its profile to ignore messages from v_i), accepts it and forwards it further, including a 'hello' back to v_i.

In Figure 7, we present an example derivation of the recipient selection protocol. Here the idea is as follows: after v_i broadcasts a 'hello' message, both v_k, v_j receive and accept the message; at this stage a recipient is selected on the basis of the reputation order between v_k and v_j, so that a new profile is built out of v_i and the higher of the two recipients, thus modelling a communication channel.

In Figure 8, we present an example derivation modelling a message passing protocol (without mistrust). Here Service 2 is a service of any kind. By the first premise in MP, the Handshaking Protocol is guaranteed terminating, including the Recipient Selection protocol if required; v_k then reads a message issued by v_i, checks for validity in its own profile through an application of trust, and if this check is passed the message is forwarded.

4. Reputation Model

In this section we illustrate the definition of the order relation $\prec$ to formalise the reputation model across vehicles, implementing the system in [15]. The main idea of

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \phi^{v_i}_{i,j} \qquad \Gamma^{v_i} \vdash_{\mathtt{s'}} Trust(\phi^{v_j}_{j,k})}{\Gamma^{v_i}; \phi^{v_j}_{j,k} \vdash_{\mathtt{max(s,s'+1)}} \phi^{v_i}_{i,j}}\text{ Weakening} \qquad \frac{\Gamma^{v_i}; \phi^{v_j}_{j,k}; \phi^{v_k}_{j,k} \vdash_{\mathtt{s}} \psi^{v_i}_{i,j} \qquad v_j \prec v_k}{\Gamma^{v_i}; \phi^{v_j}_{j,k} \vdash_{\mathtt{s+1}} \psi^{v_i}_{i,j}}\text{ Contraction}$$

$$\frac{\Gamma^{v_i}; \phi^{v_i}_{i,j}; \phi^{v_i}_{i,k} \vdash_{\mathtt{s}} \psi^{v_i}_{i,j} \qquad \phi^{v_i}_{i,j} \not\prec \phi^{v_i}_{i,k}}{\Gamma^{v_i}; \phi^{v_i}_{i,k}; \phi^{v_i}_{i,j} \vdash_{\mathtt{s+1}} \psi^{v_i}_{i,j}}\text{ Profile Exchange}$$

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} \phi^{v_i}_{i,j} \qquad \Gamma^{v_j}, \phi^{v_i}_{i,j} \vdash_{\mathtt{s'}} \phi^{v_j}_{i,k}}{\Gamma^{v_i}; \Gamma^{v_j} \vdash_{\mathtt{max(s,s')+1}} \phi^{v_j}_{i,k}}\text{ Cut}$$

Figure 4. The System `(un)SecureND`: Structural Rules

PROCEDURE `OpportunisticForwarding`(v_i, v_j)

IF v_i $Write(HELLO)$
THEN forall $[v_k \in \mathcal{A} \mid v_k\ Write(HELLO)]$,
SELECT $min(v_k, \prec)$
DO Handshaking(v_i, v_k)
ENDIF

IF Handshaking(v_i, v_k)
THEN v_i $Write(\phi_{i,k})$ AND v_k $Read(\phi_{i,k})$
IF v_k $Trust(\phi_{i,k})$
THEN v_k $Write(\phi_{i,k})$
ELSE v_k $\neg Trust(\phi_{i,k})$
ENDIFELSE
IF forall $v_i \prec v_k$, v_i $Trust(\phi_{i,k})$
THEN v_k $Trust(\phi_{i,k})$
ELSE v_k $\neg Trust(\phi_{i,k})$
ENDIFELSE
ENDIF

ENDPROCEDURE

Figure 5. Algorithm Opportunistic Forwarding

the model is the following. First, for any given message related to a service and a characteristic received from another agent (either vehicle or RSU), a vehicle will collect all the formulas that follow from accepting it, assuming each is consistent with the current profile. This is called the Feedback Set of an agent with respect to a message. Given all elements in this Feedback Set, the vehicle assigns weights to them according to the time they are received, so that the later the message, the more relevant the reaction to it. In our system, time is encoded directly by derivation steps. This is called the Vehicle's Perception with respect to a message. Next, this value is generalised to a whole set of messages concerning a service and a characteristic, by further assigning weights to each message by the relevance of the characteristic of interest, so that the higher this value the least urgent the message. We call this generalised value the Vehicle's Perception of a Characteristic Set. Hence, for each vehicle and service, a vehicle will result having higher reputation than another (with respect to a set of messages) if and only if the Perception of a Characteristic Set for that set of messages of the former is higher than that of the latter. We proceed now with the formalisation of this model.

To model the set of feedback that a given vehicle provides with respect to a given message related to a service and characteristic, we will have to collect all formulas holding following receiving a message:

Definition 5 (Feedback Set)**.** *The feedback set of vehicle v_j for a message $\phi^{v_i}_{i,j}$, for all $v_j, v_i \in \mathcal{A}$ is the set of formulas $\psi^{v_j}_{i,k}$ such that they agree with $\phi^{v_i}_{i,j}$ for the service identifier i and are obtained by a derivation construed by a $read$ rule followed by a $\rightarrow I$ rule, i.e.*

$$FS^{v_j}(\phi^{v_i}_{i,j}) = \{\psi^{v_j}_{i,k} \mid \Gamma^{v_j} \vdash_{\mathtt{s}} Read(\phi^{v_i}_{i,j}) \rightarrow \psi^{v_j}_{i,k}\}$$

By way of example, consider the simple derivation from Figure 9, which induces $FS^{v_k}(m^{v_{i,j}}_{2,1}) = \{m^{v_k}_{2,2}\}$.

Notice that, by construction, this set includes only feedback to received messages that are consistent with the current user's profile.

Definition 6 (Vehicle's Perception)**.** *The perception of vehicle v_j for a message $\phi^{v_i}_{i,j}$, for all $v_j, v_i \in \mathcal{A}$ is the sum of elements of the feedback set over that formula, weighted by the step of the derivation at which it is obtained:*

$$AP^{v_j}(\phi^{v_i}_{i,j}) = \sum_{FS^{v_i}(\phi^{v_j}_{i,k})} (\mathtt{s}(\psi^{v_j}_{i,k} \in FS^{v_i}(\phi^{v_j}_{i,k})))$$

Intuitively, the value of $\mathtt{s}$ at each step of each derivation leading to each formula in the feedback set of a vehicle to a given service and characteristic is summed up to provide a value that increases linearly to reflect a step value for a time function. The value of $AP^{v_j}(\phi^{v_i}_{i,j})$ will reflect the aggregation of all the feedback provided on each characteristics of a given service.

We can now generalise to the set of all feedback on a characteristic for a given service, remembering that these are given in a preorder so that the position of the characteristic in that order is mapped into an integer:

Definition 7 (Vehicle's Perception of Characteristic Set)**.** *The perception of vehicle v_j for a set of messages $\mathcal{M}^{\mathcal{A}}_{S_i,C_k}$ from other vehicles about characteristic C_k of service S_i is the sum of elements of the feedback set over the messages received about that service characteristic, weighted by the steps of the derivation at which it is obtained and further by the value $\mathtt{r}(C_k)$ of the rank of characteristic k:*

$$AP^{v_j}(\mathcal{M}^{\mathcal{A}}_{S_i,C_k}) = \sum_{FS^{v_i}(\phi^{v_j}_{i,k} \dots \phi^{v_n}_{i,k})} (1 - \mathtt{r}(C_k)(\mathtt{s}(\psi^{v_j}_{i,k} \in FS^{v_i}(\phi^{v_j}_{i,k} \dots \phi^{v_n}_{i,k}))))$$

Using the vehicle's perception of characteristic set, we can define the order of reputation with respect to services

$$\dfrac{\Gamma^{v_i} : profile \qquad \Gamma^{v_i} \vdash_1 hello^{v_i}_{1,1}}{\Gamma^{v_i} \vdash_2 Write(hello^{v_i}_{1,1})} \text{ Hello Message}$$

$$\dfrac{\Gamma^{v_i} \vdash_1 Write(hello^{v_i}_{1,1}) \qquad \Gamma^{v_k} \vdash_2 Read(hello^{v_i}_{1,1}) \qquad \Gamma^{v_k}; hello^{v_i}_{1,1} : profile}{\Gamma^{v_k}; hello^{v_i}_{1,1} \vdash_3 Write(hello^{v_k}_{1,1})} \text{ Response Message}$$

Figure 6. The Handshaking Protocol

$$\dfrac{\Gamma^{v_{j,\dots,n}}; hello^{v_i}_{1,1} \vdash_1 Write(hello^{v_{j,\dots,n}}_{1,1}) \qquad v_l \in min(v_{i,\dots,n}, \prec)}{\Gamma^{v_i}; \Gamma^{v_l} : profile} \text{ Recipient Selection}$$

Figure 7. The Handshaking Protocol

$$\dfrac{\dfrac{\dfrac{\Gamma^{v_i}; \Gamma^{v_k} : profile \qquad \Gamma^{v_i} \vdash_1 Write(m^{v_i}_{2,1})}{\Gamma^{v_k} \vdash_2 Read(m^{v_i}_{2,1})} \text{ MP} \qquad \Gamma^{v_k}; m^{v_i}_{2,1} : profile}{\Gamma^{v_k} \vdash_3 Trust(m^{v_i}_{2,1})}}{\Gamma^{v_k} \vdash_4 Write(m^{v_i}_{2,1})}$$

Figure 8. The Message Passing Protocol

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma^{v_i}; \Gamma^{v_k} : profile \qquad \Gamma^{v_j}; \Gamma^{v_k} : profile}{\Gamma^{v_i}; \Gamma^{v_j}; \Gamma^{v_k} : profile} \qquad \Gamma^{v_k} \vdash_1 Write(m^{v_{i,j}}_{2,1})}{\Gamma^{v_k} \vdash_2 Read(m^{v_{i,j}}_{2,1})} \qquad \Gamma^{v_k}; m^{v_{i,j}}_{2,1} : profile}{\Gamma^{v_k} \vdash_3 Trust(m^{v_{i,j}}_{2,1})}}{\Gamma^{v_k} \vdash_4 Write(m^{v_{i,j}}_{2,1})} \qquad \Gamma^{v_k}; m^{v_{i,j}}_{2,1} \vdash_5 m^{v_k}_{2,2}}{\Gamma^{v_k} \vdash_6 m^{v_i}_{2,1} \to m^{v_k}_{2,2}}$$

Figure 9. An Example Feedback Set

and characteristics, which establishes a higher position for the vehicle whose perception on the characteristics set for that Service is greater.

Definition 8 (Reputation)**.** $\forall v_i, v_j \in \mathcal{V}, S_i \in \mathcal{S}, v_i \prec v_j \leftrightarrow AP^{v_i}(\mathcal{M}^{\mathcal{A}}_{S_i,C_k}) > AP^{v_j}(\mathcal{M}^{\mathcal{A}}_{S_i,C_k})$.

5. Conclusions

In this paper we have formulated a proof-theory for trust and reputation in VANETs. Our language is modelled on the logic `(un)SecureND`, including an explicit $trust$ function on formulas to guarantee consistency check at each retrieval step (after a $read$ function), before forwarding is granted for a package (by a $write$ function). Forwarding is modelled in an opportunistic fashion, selecting receivers on the basis of their reputation ranking. Trust on forwarding also guarantees correctness on transitive transmissions. Moreover, reputation is used to implement the resolution protocol for restoring information after removing previously stored data. Several improvements for the algorithm are possible, including majority selection on opportunistic forwarding (instead of consensus) and separate ordering for vehicles and RSUs. Validation of the system is obtained by implementation of the `(un)SecureND` calculus as a large inductive type in the Coq proof assistant. The development is available at https://github.com/gprimiero/SecureNDC. A characteristic of the logic `(un)SecureND` is its substructural nature, which in future work can be exploited to investigate cases of strengthened and limited resource redundancy for fault tolerance and source shuffling for security. Other applications of negative trust can be investigated to distinguish between malevolent and simply unsuccessful sources.

Acknowledgement. Taolue Chen is partially supported by UK EPSRC grant (EP/P00430X/1) and European CHIST-ERA project SUCCESS.

References

[1] Mohamed Salah Bouassida. Authentication vs. privacy within vehicular ad hoc networks. *International Journal of Network Security*, 13(3):121–134, 2011.

[2] Brijesh Kumar Chaurasia, Ranjeet Singh Tomar, and Shekhar Verma. Using trust for lightweight communication in VANETs. *IJAISC*, 5(2):105–116, 2015.

[3] John Finnson, Jie Zhang, Thomas T. Tran, Umar Farooq Minhas, and Robin Cohen. A Framework for Modeling Trustworthiness of Users in Mobile Vehicular Ad-Hoc Networks and Its Validation through Simulated Traffic Flow. In *User Modeling, Adaptation, and Personalization - 20th International Conference, UMAP 2012.*

Proceedings, volume 7379 of *Lecture Notes in Computer Science*, pages 76–87. Springer, 2012.

[4] Félix Gómez Mármol and Gregorio Martínez Pérez. TRIP, a Trust and Reputation Infrastructure-based Proposal for Vehicular Ad Hoc Networks. *J. Netw. Comput. Appl.*, 35(3):934–941, May 2012.

[5] M. H. Jahanian, F. Amin, and A. H. Jahangir. Analysis of tesla protocol in vehicular ad hoc networks using timed colored petri nets. In *2015 6th International Conference on Information and Communication Systems (ICICS)*, pages 222–227, April 2015.

[6] Savas Konur and Michael Fisher. Formal Analysis of a VANET Congestion Control Protocol through Probabilistic Verification. In *Proceedings of the 73rd IEEE Vehicular Technology Conference, VTC Spring 2011, 15-18 May 2011, Budapest, Hungary*, pages 1–5. IEEE, 2011.

[7] Ku, I., Lu, Y., Gerla, M., Gomes, R. L., Ongaro, F. and Cerqueira, E. Towards software-defined VANET: Architecture and services. In *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, pp. 103-110, 2014.

[8] Nai-Wei Lo and Hsiao-Chien Tsai. A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks. *EURASIP Journal on Wireless Communications and Networking*, 2009(1):125348, 2009.

[9] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen. A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 41(3):407–420, May 2011.

[10] Giuseppe Primiero. A Calculus for Distrust and Mistrust. In *Trust Management X - 10th IFIP WG 11.11 International Conference, IFIPTM, Proceedings*, volume 473 of *IFIP Advances in Information and Communication Technology*, pages 183–190. Springer, 2016.

[11] Giuseppe Primiero and Franco Raimondi. A typed natural deduction calculus to reason about secure trust. In Ali Miri, Urs Hengartner, Nen-Fu Huang, Audun Jøsang, and Joaquín García-Alfaro, editors, *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, pages 379–382. IEEE, 2014.

[12] Maxim Raya, Panagiotis Papadimitratos, Virgil D. Gligor, and Jean-Pierre Hubaux. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In *INFOCOM*, pages 1238–1246. IEEE, 2008.

[13] Greg Restall. *An Introduction to Substructural Logics*. Routledge, 2000.

[14] Seyed Ahmad Soleymani, Abdul Hanan Abdullah, Wan Haslina Hassan, Mohammad Hossein Anisi, Shidrokh Goudarzi, Mir Ali Rezazadeh Baee, and Satria Mandala. Trust management in vehicular ad hoc network: a systematic review. *EURASIP Journal on Wireless Communications and Networking*, 2015(1):146, 2015.

[15] R Vanni, L.M.S. Jaimes, G. Mapp, and E. Moreira. Ontology Driven Reputation Model for VANET. In *AICT 2016, The Twelfth Advanced International Conference on Telecommunications* , pages 14–19. IARIA, 2016.

[16] Yu-Chih Wei and Yi-Ming Chen. *Reliability and Efficiency Improvement for Trust Management Model in VANETs*, pages 105–112. Springer Netherlands, Dordrecht, 2012.

[17] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmüller, and Luca Delgrossi. Trust Issues for Vehicular Ad Hoc Networks. In *Proceedings of the 67th IEEE Vehicular Technology Conference, VTC Spring 2008, 11-14 May 2008, Singapore*, pages 2800–2804. IEEE, 2008.