A Proof-theoretic Trust and Reputation Model for VANET

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

Abstract—**Vehicle Ad Hoc Networks (VANETs) are becoming an important part of intelligent transportation systems. In this context, security requirements need to rely on a combination of agents' reputation and trust relations over the messaging infrastructure, in order to maintain a dynamic and safe behaviour evaluation. 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, with potentially disastrous effects. In this paper we provide a proof-theoretic interpretation of a reputation and trust model for VANET, which allows for a formal verification through translation into the Coq proof assistant, and which guarantees consistency of messaging protocols and security of transitive transmissions.**

1. Introduction

Vehicle Ad Hoc Networks (VANETs) consist of vehicles and roadside units networks created to enhance transportation systems through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. 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 [13] for a recent overview. Trust models in VANETs differ in accordance to the main object of the model: entity-centric [8], [4], data-centric [11], [7] and combined [15]. Among the models that combine trust and reputation, the work in [14] gives an analysis that accounts for reputation as a characteristic of message forwarding, as well as vehicles, drivers and other agents: here reputation is therefore based on a descriptive ontology of the model and is used to provide feedback in the system. An overview of the issues related to the trust in fixed and mobile ad hoc networks is given in [16], 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. Yet, 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 checkable. 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; privacy and authentication are verified using the AVISPA tool in [1], while the TESLA authentication protocol is verified in [5] using Petri nets. None of these (few) approaches 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.

The present paper provides a solution to both problems mentioned above. In Section 2 we formulate a proof-theoretic translation of the trust and reputation model for VANET given in [14] in an extension of the natural deduction calculus (un)SecureND from [9]. The aim is, first of all, to show that the trust properties instantiated through our calculus faithfully reflect those in a VANET network; accordingly, we show how non-trustworthy interactions can be proven to be such 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 normalization result. 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 feedback messages parametrised, in view of a temporal measure and a ranking of the relevant service characteristic of the message.

2. (un)SecureND

(un)SecureND is a natural deduction calculus defining trust, mistrust and distrust protocols introduced in [10] for the positive fragment and in [9] for the negation complete extension. Here we provide a slightly modified version adapted for a VANET network. In particular, the present version introduces: 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 our logic:

Definition 1 (Syntax of (un)`SecureND`).

$$
\begin{aligned}
&\mathcal{A}^{\prec} := \{\mathcal{V}, \mathcal{R}\}\\
&\mathcal{V} := \{v_1 \prec \ldots \prec v_n\}\\
&\mathcal{R} := \{rsu_1 \prec \ldots \prec rsu_n\}\\
&\mathcal{S} := \{S_1, \ldots, S_n\}\\
&\mathcal{C} := \{C_1 \leq \cdots \leq C_n\}\\
&\phi^{\mathcal{A}}_{S_i,C_j} := a^{\mathcal{A}}_{S_i,C_j} \mid \neg\phi^{\mathcal{A}}_{i,j} \mid \phi^{\mathcal{A}}_{i,j} \rightarrow \phi^{\mathcal{A}}_{k,l} \mid \phi^{\mathcal{A}}_{i,j} \wedge \phi^{\mathcal{A}}_{k,l}\\
&\qquad\qquad \mid \phi^{\mathcal{A}}_{i,j} \vee \phi^{\mathcal{A}}_{k,l} \mid \bot\\
&mode := Read(\mathcal{M}^{\mathcal{A}}) \mid Write(\mathcal{M}^{\mathcal{A}}) \mid Trust(\mathcal{M}^{\mathcal{A}})\\
&RES := \mathcal{M}^{\mathcal{A}} \mid mode \mid \neg RES\\
&\Gamma^{\mathcal{A}} := \phi^{\mathcal{A}}_{i,j} \mid \phi^{\mathcal{A}}_{i,j} < \phi^{\mathcal{A}}_{k,l} \mid \Gamma^{\mathcal{A}}; \phi^{\mathcal{A}}_{i,j}
\end{aligned}
$$

$\mathcal{A}$ is the set of agents issuing messages and including vehicles $\mathcal{V}$ and roadside units (RSUs) $\mathcal{R}$. Below we will focus in particular on V2V communication, without loss of generality. $\mathcal{S}$ and $\mathcal{C}$ denote sets of services and their characteristics, respectively. 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, which are of the form $\phi^{v_i}_{S_k,C_j}$, which intuitively expresses a message ϕ about service S_k and characteristic C_j, generated by vehicle v_i. When required, we will refer to a set of messages about service S_k and characteristic C_k from agent v_i as $\mathcal{M}^{v_i}_{S_i,C_k}$; this notation can be further generalised to a whole set of agents $\{v_i, \ldots, v_k\} \subseteq \mathcal{A}$. We assume here and throughout that characteristics $\mathcal{C}$ of services are given as posets and their ordering is used to order messages below in Definition 4. To simplify notation, a message $\phi^{v_i}_{S_k,C_j}$ is usually abbreviated as $\phi^{v_i}_{k,j}$. $mode$ is a variable for reading, writing and trusting messages, closed under negation. An agent profile $\Gamma^{\mathcal{A}}$ is the current list of all messages collected by the agent either from other agents or from various available sensors and other networks. For the present purposes, the latter ones will be indexed at their first vehicle or RSU collecting it, so as not to add networks as separate agents.

Definition 2 (Formulae). *A formula $\Gamma^{v_l} \vdash_{\mathtt{s}} \phi^{v_j}_{i,k}$ 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 formula $\vdash_{\mathtt{s}} \phi^{v_j}_{i,k}$ says that a message ϕ about service i and characteristic k signed from agent v_j holds for any agent's profile at step* $\mathtt{s}$.

Messages satisfy a ranking based on characteristics:

Definition 4. *An order between messages $\phi^{v_j}_{i,k} < \phi^{v_j}_{i,l}$ holds if $C_k \leq C_l \in S_i$ for an agent v_j.*

The order relation between service characteristics induces therefore validity under profile: if a characteristic i is essential to another one l with respect to a service i for an agent v_j, then that agent will be required to obtain a value for i in order to validly access a value for l.

A valid agent profile meets all the requirements and conflicts clauses of all service messages that the user collects. Rules from Figure 1 define agent's profile construction from service messages requirements. By Empty Profile, a user profile can be empty (base case); by Message Insertion, the elements in an installation profile are messages; 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.

2.1. Rules for message construction

The operational rules in Figure 2 formulate compositionality of messages. The rule $Atom$ establishes valid content within a user profile and across other profiles with satisfied requirements. $\bot$ formulates implication of access to contradictory messages, in which case the profile must be consistent with the negated access. $\wedge$-I allows message composition from distinct profiles; by $\wedge$-E, each composing message can be obtained from the combined profiles. $\vee$-I says that a combined profile can access any message produced from each of the composing profiles; by the elimination $\vee$-E, each message consistently inferred by each individual profile can also be executed under the extended profile. $\rightarrow$-Introduction expresses inference of a message from a combined profile as inference between messages (Deduction Theorem); its elimination $\rightarrow$-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 an agent's profile to act on messages from a distinct agent. $\neg$-distribution expresses profile consistency: if an agent's profile does not allow inferring a message $\phi_{i,j}$, then it allows inferring any other message whose requirements do not include $\phi_{i,j}$. $read$ says that from any consistent profile a message can be read provided its requirements are satisfied (if any). $trust$ works as an elimination rule for $read$: it says that if a message is received and it preserves profile consistency, then it can be trusted. $write$ works as an elimination rule for $trust$: it says that a readable and trustable message can be broadcast. $exec$ says that every message consistently received by a profile is valid in it. The rule MTrust-I says that currently held message conflicting with a newly arrived message are mistrusted, i.e. removed from the current 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 user profile, including any required dependency, as expressed by the side condition that requires checking with any other agent who has higher reputation than the sender of the original message. The side condition can be modified at will, e.g.,

$$\frac{}{\{\} : profile}\ \text{Empty Profile} \qquad \frac{\phi^{v_j}_{i,k} : \mathcal{M}^{v_j}}{\phi^{v_j}_{i,k} : profile}\ \text{Message Insertion}$$

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

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

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

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

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

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

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

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

to design a protocol that will restore previous information if a sufficient number of other agents with higher reputation support it. *mistrust* is a flag for facilitating removal of messages present in the user 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 [12]. Weakening is constrained by an instance of *trust*: it says that valid information is preserved under an agent's profile extension, assuming the latter is provably consistent and therefore no refresh is required. Contraction is constrained by preservation of ordering: it says that removing identical messages from an agent's profile is admissible, with the constraint that the copy from the agent 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 profile extension: if a message $\phi_{i,j}$ is validly for agent 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 (Normalization)**.** *Any* (un)`SecureND` *derivation with an occurrence c of the Cut rule can be transformed into another derivation with the same end sequent 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 Weakenings 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. □

Normalization 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.

3. Opportunistic Forwarding

In Figure 5 we present an example derivation for a simple handshaking protocol. Here Service 1 identifies the set of messages for this protocol. By Hello Message, a user

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

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

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

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

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

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

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

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

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

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

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 ingore messages from v_i), accepts it and forwards it further, including a 'hello' back to v_i.

In Figure 6, 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 7, we present an example derivation modelling a message passing protocol (without mistrust). Here Service 2 is some 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.

The full protocol with handshaking and opportunistic forwarding is formulated in Figure 8.

4. Reputation Model

In this section we illustrate the definition of the order relation $\prec$ to formalise the reputation model across agents. Higher reputation is modelled by feedback aggregation. Our system integrates the elements of the main feedback 6-tuple function from [14]. In particular, time is encoded directly by derivation steps; context is embedded by the user profile; service and characteristics are modelled by messages. To model the set of feedback that a given agent provides with respect to a given message related to a service and characteristic, we will have to collect all formulae following receiving a message:

Definition 5 (Feedback Set). *The feedback set of agent 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 $\to I$ rule, i.e.*

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

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

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

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

Figure 5. The Handshaking Protocol

$$\frac{\Gamma^{v_k}; hello^{v_i}_{1,1} \vdash_1 Write(hello^{v_k}_{1,1}) \qquad \Gamma^{v_j}; hello^{v_i}_{1,1} \vdash_2 Write(hello^{v_j}_{1,1}) \qquad v_k \prec v_j}{\Gamma^{v_i}; \Gamma^{v_k} : profile}\text{Recipient Selection}$$

Figure 6. The Handshaking Protocol

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

Figure 7. The Message Passing Protocol

```
PROCEDURE OpportunisticForwarding($(v_i, v_j)$)

FOR $(v_i, v_j, v_k) \in \mathcal{A}$
    IF $v_i Write(HELLO)$
        THEN forall $v_j, v_k \in \mathcal{A}$,
               $v_j Write(HELLO)$ AND $v_k Write(HELLO)$
                IF $v_j \prec v_k$
                  THEN $v_i, v_j$
                  DO Handshaking
                  ELSE $v_i, v_k$
                  DO Handshaking
               ENDIFELSE
    ENDIF

    IF Handshaking($v_i, v_j$)
      THEN $v_i Write(S, C)$ AND $v_j Read(S, C)$
          IF $v_j Trust(S, C)$
            THEN $v_j Write(S, C)$
            ELSE $v_j MTrust(SC)$
                  IF forall $v_i \prec v_j$, $v_i Trust(SC)$
                    THEN $v_j Trust(SC)$
                    ELSE $v_j \neg Trust(S, C)$
                  ENDIFELSE
            ENDIFELSE
          ENDIF
        ENDIF

  ENDFOR
ENDPROCEDURE
```

Figure 8. Algorithm Opportunistic Forwarding

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

Definition 6 (Agent's Perception)**.** *The perception of agent 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 an agent 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 (Agent's Perception of Characteristic Set)**.** *The perception of agent v_j for a set of messages $\mathcal{M}^{\mathcal{A}}_{S_i,C_k}$ from agents in $\mathcal{A}$ 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 agent's perception of characteristic set, we can define the order of reputation with respect to services and characteristics, which establishes a higher position for the agent whose perception on the characteristics set for that Service is greater.

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

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

Figure 9. An Example Feedback Set

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.

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 Judith Masthoff, Bamshad Mobasher, Michel C. Desmarais, and Roger Nkambou, editors, *User Modeling, Adaptation, and Personalization - 20th International Conference, UMAP 2012, Montreal, Canada, July 16-20, 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] 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.

[8] 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.

[9] Giuseppe Primiero. A Calculus for Distrust and Mistrust. In Sheikh Mahbub Habib, Julita Vassileva, Sjouke Mauw, and Max Mühlhäuser, editors, *Trust Management X - 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings*, volume 473 of *IFIP Advances in Information and Communication Technology*, pages 183–190. Springer, 2016.

[10] 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, Toronto, ON, Canada, July 23-24, 2014*, pages 379–382. IEEE, 2014.

[11] 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.

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

[13] 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.

[14] 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.

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

[16] 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.