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
www.cs.mdx.ac.uk/people/giuseppe-primiero/

Paris, 30/04/2017

Vehicular Ad Hoc Networks (VANETs)

- vehicles and roadside unit networks created to enhance transportation systems: `http://www.vanet.mdx.ac.uk/`
- vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications
- services include:
  - vehicle and road safety services
  - traffic efficiency and management services
  - information and entertainment services.

Trust

Trust to ensure integrity, reliability and safety of services.

- entity-centric trust [9, 4]
- data-centric [12, 8]
- combined [16].
- overview of trust in fixed and mobile ad hoc networks [17],

Reputation

- [15]: offers an analysis as a characteristic of message forwarding among vehicles, drivers and other agents:
- other approaches in [3, 2].

Current Apporaches to Verification

- simulations cannot guarantee the absence of unpredictable and unsafe behaviours
- exhaustive safety control is through formal verification
- Formal approaches to VANET include
  - [6] for verification of a congestion control protocol using PRISM
  - verification of privacy and authentication using the AVISPA tool in [1];
  - verification of the TESLA authentication protocol [5] using Petri nets.
- theorem proving ignored so far

Objectives

1. proof-theoretic translation of the trust and reputation model for VANET given in [15]
2. identify non-trustworthy relations through a proof-checking method
3. calculus formally correct through translation to a Coq library.
4. transitive message passing operations are guaranteed safe
5. protocols for handshaking, recipient selection and message passing based on reputation

Definition (Syntax of (un)SecureND)

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

Examples

> *A vehicle profile* Γ^{v_i} *receives a message* $\phi_{j,k}$ *about service* $S_j = \texttt{weather}$ *and characteristic* $C_k = \texttt{temperature}$ *stating* $\phi = (temp \geq 5^\circ C)$.

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* $\texttt{weather}$, $C_k = \texttt{humidity}$ *and* $C_l = \texttt{precipitation} - \texttt{forecast}$, *where the former characteristic is essential to determine the latter.*

Judgement

Definition (Judgements)

A judgement $\Gamma^{v_l} \vdash_{\mathbb{s}} \phi_{i,k}^{v_j}$ states that a message ϕ about service i and characteristic k signed from agent v_j is validly accessed at step $\mathbb{s} \geq 0$ under the profile of agent v_l.

Access Rules

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

$$\frac{}{\Gamma^{v_i} \vdash_{\mathtt{s}} Read(\psi_{i,l}^{v_j})}\ read$$

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

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

$$\frac{\Gamma^{v_i} \vdash_{\mathtt{s}} Write(\psi_{i,l}^{v_j})}{\Gamma^{v_i} \vdash_{\mathtt{s}+1} \psi_{i,l}^{v_j}}\ exec$$

Checking for inconsistent messages

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

Accepting new (inconsistent) information

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

Opportunistic Forwarding

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

Reacting to messages

Definition (Feedback Set)

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

$$FS^{v_j}(\phi_{i,j}^{v_i}) = \{\psi_{i,k}^{v_j} \mid \Gamma^{v_j} \vdash_{s} Read(\phi_{i,j}^{v_i}) \rightarrow \psi_{i,k}^{v_j}\}$$

Assessing messages' value based on time

Definition (Vehicle's Perception)

The perception of vehicle v_j for a message $\phi_{i,j}^{v_i}$, 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:

$$AP^{v_j}(\phi_{i,j}^{v_i}) = \sum_{FS^{v_i}(\phi_{i,k}^{v_j})} (\mathbf{s}(\psi_{i,k}^{v_j} \in FS^{v_i}(\phi_{i,k}^{v_j})))$$

Assessing messages' set value based on time and ranking

Definition (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:

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

where $\mathtt{r}$ is a ranking of characteristics valid for each vehicle v_i.

Vehicles' reputation based on the value of their messages

Definition (Reputation)

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

Conclusions

- a proof-theory for trust and reputation in VANETs
- 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 message (by a *write* function).
- Opportunistic Forwarding selects receivers on the basis of their reputation ranking
- Trust on forwarding guarantees correctness on transitive transmissions
- resolution protocol for restoring information after removing previously stored data.
- Protocol Validation via as a large inductive type in the Coq proof assistant `https://github.com/gprimiero/SecureNDC`.
- Future Work:
  - majority selection on opportunistic forwarding (instead of consensus)
  - separate ordering for vehicles and RSUs.

Refrences I

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

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

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.

Refrences II

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.

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.

Refrences III

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.

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.

Refrences IV

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.

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.

Refrences V

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.

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.

Refrences VI

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.

Greg Restall.
An Introduction to Substructural Logics.
Routledge, 2000.

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.

Refrences VII

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.

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

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.