Fully Distributed Trust Management Scheme for Vehicular Networks

Renan Domingos M. Greca, Luiz Carlos P. Albini

[1]Informatics Department – Federal University of Paraná
PoBox: 19081 – 81.531-980 – Curitiba – PR – Brazil

rdmgreca@inf.ufpr.br, albini@ufpr.br

Google Contact: Lucas Radaelli

Abstract. *By integrating processors and wireless communication units into vehicles, it is possible to create a vehicular communication network, in which cars share data, such as speed and position, amongst themselves in order to cooperate and make roads safer and more efficient. Vehicular communication networks are the first step to implement Smart Cities technological solutions for road safety. However, as is the case with most new technologies, these networks might be a prime target for attacks performed by malicious users, who may benefit from affecting traffic conditions. In order to avoid such attacks, one important feature for vehicular networks is trust management. It allows nodes to filter incoming messages according to previously established trust values assigned to other nodes. This work proposes a trust management model in the context of daily commutes, taking advantage of social features that can be found in vehicular networks.*

1. Goals and problem statement

Considering the high speed and potentially life-threatening situations of vehicular networks, it is essential for messages to be delivered with low latency, which is why a fully distributed approach is preferred. Due to the highly dynamic scenario, it is also important that the message delivery does not depend on pre-defined infrastructures. Therefore, ad-hoc networks might correctly fit this paradigm, creating a Vehicular Ad-Hoc Network (VANET). It does not rely on an Internet connection or existing infrastructure, meaning that all network services depend on the participating vehicles themselves. However, it also means that any vehicle can join the network by being within the communication range. While this is expected, as VANETs benefit from having more participants, it can be a problem when one or more members of the network turn out to be malicious. Malicious nodes are ones that share falsified or otherwise incorrect information with other members, which can in turn cause traffic jams or even accidents. One way of avoiding the dissemination of false data is to have nodes assign trust values to other nodes. As they interact and observe each other's behaviors, nodes can decide whether or not data sent from others is reliable.

To create and maintain long-term trust relationships with one another, nodes in a vehicular network must have a reasonable chance of interacting somewhat frequently. Although it cannot be expected that all pairs of nodes satisfy this requirement, there are social aspects observed in vehicular networks which show that, at least for some pairs of nodes, encounters can happen relatively frequently [Cunha et al. 2014]. For example, vehicles belonging to family members, neighbors or workmates are very likely parked close to each other almost every day. Furthermore, vehicles that perform daily commutes,

as well as public transit vehicles like buses, are expected to travel along the same roads at around the same time every day.

Using these long term relationships, nodes can generate trust values and models of their surroundings. This information can be represented as a graph in which vertices are vehicles and edges are trust relationships between pairs of vehicles. Information collected from previous encounters with known nodes can be used to estimate some of the edges in the model; meanwhile, further information can be extracted from neighboring nodes and ongoing encounters, filling out the remainder of the graph.

The goal of this work is to develop a trust management algorithm, which can be used to efficiently detect malicious nodes on the network. This work is an extension of [Vernize et al. 2015], which introduces the fastest and most precise malicious node identification mechanism based on trust management for centralized static social networks. This work will extend such trust management to dynamic and distributed vehicular networks.

2. Expected work and outcomes

There are three main components of the proposed work.

First, [Vernize et al. 2015] will be extended to serve a dynamic and decentralized network. The main differences between the two approaches are: (1) the graph used as input is incomplete, as nodes only have partial knowledge of the network; (2) instead of a single graph, there will be multiple variations of it, for each node and for each moment in time; and (3) trust will be measured in a range of $[0, 1]$, instead of being binary.

Second, the evaluation will be made through simulations using the Working Day Movement Model [Ekman et al. 2008]. The model was developed for mobile devices (such as smartphones) being carried by humans, so it must be adapted to suit a vehicular network. Finally, results will be analyzed to confirm the algorithm's efficiency and effectiveness.

3. Previous work

Several trust management models for vehicular networks have been proposed, with different degrees of success. Some of them emphasize *entity-based trust*, in which trust values are stored for each node and that value is used to judge messages originating from it. This has the advantage of shortening evaluation time for each message delivered, since most trust information is previously obtained. Others use *data-oriented trust*, in which messages are individually evaluated regardless of the sender. These solutions are useful when nodes are mostly strangers to one another and must quickly decide whether or not to trust an incoming alert sent by an unknown source.

VARS [Dotzer et al. 2005] is an early example of a VANET trust model, using a process the authors call opinion piggybacking. That is, when an event occurs and a node broadcasts an alert message about it, other nodes append their opinion on both the message contents and the message sender onto the alert. Therefore, nodes receive a combined opinion of several of its neighbors, helping it to form its own decision. However, this process has privacy implications in case the message is not of public service, and the opinion piggybacking itself might add unnecessary latency and overhead to the broadcast.

The model in [Chen et al. 2010] proposes the formation of clusters of nodes, in which one leader aggregates the other nodes' opinions about each message sent. It is exceedingly costly to maintain clusters in a highly dynamic network, and might be unfeasible if the network is too sparse to generate relevant clusters.

[Park et al. 2011] uses daily commutes and road-side units (stationary equipment which may act as part of a VANET). Each vehicle is assigned an "Agent RSU", which is responsible for maintaining the vehicle's trust value and sharing it with others. The trust value maintenance is comparable to the one proposed here, although it relies heavily on existing infrastructure, which is not always reasonable.

In [Huang et al. 2014], authors identify features generally associated with social networks and use them to generate a VANET trust model. The algorithm places heavy emphasis on the opinion of the nodes in which messages originate, which may be a problem if those nodes are malicious. Nevertheless, there is no trust management scheme for VANETs which take advantage of the users' long term relationship as the one proposed here.

4. Data Policy

Once the research is concluded, all related code and datasets will be available online in an open-source fashion. Along with the dissertation required for the Master of Science degree, articles will be published explaining the core methodology, algorithms and experiments performed.

References

Chen, C., Zhang, J., Cohen, R., and Ho, P.-H. (2010). A trust modeling framework for message propagation and evaluation in vanets. In *Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on*, pages 1–8. IEEE.

Cunha, F. D., Vianna, A. C., Mini, R. A., and Loureiro, A. A. (2014). Is it possible to find social properties in vehicular networks? In *Computers and Communication (ISCC), 2014 IEEE Symposium on*, pages 1–6. IEEE.

Dotzer, F., Fischer, L., and Magiera, P. (2005). Vars: A vehicle ad-hoc network reputation system. In *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, pages 454–456. IEEE.

Ekman, F., Keränen, A., Karvo, J., and Ott, J. (2008). Working day movement model. In *Proceedings of the 1st ACM SIGMOBILE workshop on Mobility models*, pages 33–40. ACM.

Huang, Z., Ruj, S., Cavenaghi, M. A., Stojmenovic, M., and Nayak, A. (2014). A social network approach to trust management in vanets. *Peer-to-Peer Networking and Applications*, 7(3):229–242.

Park, S., Aslam, B., and Zou, C. C. (2011). Long-term reputation system for vehicular networking based on vehicle's daily commute routine. In *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, pages 436–441. IEEE.

Vernize, G., Guedes, A. L. P., and Albini, L. C. P. (2015). Malicious nodes identification for complex network based on local views. *The Computer Journal*, 58(10):2476–2491.

Luiz Carlos Pessoa Albini
Federal University of Paraná - Informatics Department
R. Cel. Francisco H. dos Santos, 100 - Centro Politécnico - PoBox 19081 - 81531-980
Curitiba - PR - Brazil
Phone: +55-41-33613412
e-mail: albini@ufpr.br

Education

Degree in Computer Science at Federal University of Paraná in 1998 – Brazil

Masters Degree in Computer Science at Federal University of Paraná in 2000 – Brazil

PhD in Computer Science at Pisa University 2004 – Italy

University Activities

Associate Professor at Federal University of Paraná since 2006

Lectures for Graduate and Undergraduate Courses:

- Computer Networks
- Cryptography
- Wireless Networks
- Digital Circuits
- Algorithm

Tutoring:

- 12 Masters Dissertations
- 2 PhD Thesis

On-going tutoring:

- 6 Masters Students
- 2 PhD Students

On-Going Research Projects

Internet of Things

- Secure Middleware
- 2 PhD Students

Vehicular Networks

- Security Routing
- Trust Management

Cryptography

- Proxy-Based Cryptography for e-Health
- Parallel Prime Number Generator
- Key Management for Delay Tolerant Networks

Reviewer Activities

Project Reviewer for:

- Framework 7 – European Commission
- Consultative Committee for Space Data Systems
- Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) - Brazil
- Fondo Nacional de Desarrollo Científico y Tecnológico (Fondecyt) - Chile
- Fundação Araucária – Brazil

Journal Reviewer:

- IEEE Communications Letters – ISSN: 1089-7798
- The Journal of Systems and Software – ISSN: 0164-1212
- IET Communications – ISSN: 1751-8628
- Network Protocols and Algorithms – ISSN: 1943-3581
- International Journal of Distributed Sensor Networks – ISSN: 1550-1477
- Journal of Computer Networks and Communications – ISSN: 2090-7141
- IEEE Transactions on Computers – ISSN: 0018-9340
- Computer Networks – ISSN: 1389-1286
- Revista do IEEE América Latina – ISSN: 1548-0992
- Journal of Network and Systems Management – ISSN: 1573-7705

Research

Published 22 articles in international journals
Published 31 papers in national and international congress and symposium
Citations:

- Web of Science - Articles:19 - Citations:26
- SCOPUS - Article:31 - Citations:155
- Google Schoolar – Article:54 - Citations:374

Main Recent Journal Publications:

- de Araujo Zanella, Angelita; Albini, Luiz Carlos P. A Reed-Solomon Based Method to Improve Message Delivery in Delay Tolerant Networks. *International Journal of Wireless Information Networks*, v. 1, p. 1-10, 2017.
- da Silva, Eduardo; Albini, Luiz Carlos P. SEMAN: A Novel Secure Middleware for Mobile Ad Hoc Networks. *Journal of Computer Networks and Communications*, v. 2016, p. 1-18, 2016.
- da Silva, Eduardo; Albini, Luiz Carlos P. Middleware proposals for mobile ad hoc networks. *Journal of Network and Computer Applications*, v. 43, p. 103-120, 2014.
- Menegazzo, Cinara; Albini, Luiz Carlos P. Unadvertised energy saving method for static and homogeneous wireless sensor networks. *IET Wireless Sensor Systems*, v. 4, p. 105-111, 2014.
- Vernize, Grazielle; Guedes, André L. P.; Albini, Luiz Carlos P. Malicious Nodes Identification for Complex Network Based on Local Views. *Computer Journal (Print)*, v. 1, p. 1, 2014.
- Misaghi, Mehran; da Silva, Eduardo; Albini, Luiz Carlos P. Distributed Self-organized Trust Management for Mobile Ad Hoc Networks. *Communications in Computer and Information Science (Print)*, v. 293, p. 506-518, 2012.
- da Silva, Eduardo; Misaghi, Mehran; Albini, Luiz Carlos P. TRUE: a trust evaluation service for Mobile Ad Hoc Networks resistant to malicious attacks. *Journal of Digital Information Management*, v. 10, p. 262-271, 2012.
- da Silva, Eduardo; Silva, Renan F.; Albini, Luiz Carlos. P. Security Through Virtualization on Mobile Ad Hoc Networks. *International Journal on Communications Antenna and Propagation*, v. 2, p. 270-275, 2012.
- Duarte, Elias P.; Ziwich, Roverli P.; Albini, Luiz Carlos P. A survey of comparison-based system-level diagnosis. *ACM Computing Surveys*, v. 43, p. 1-56, 2011.
- Nogueira, Michele; da Silva, Eduardo; Albini, Luiz Carlos P.; Santos, Aldri L. Survivable key management on WANETs. *IEEE Wireless Communications*, v. 18, p. 82-88, 2011.