August 31st 2018.
T-SET Final Report

A Model for Enabling Trustworthiness in V2V Networks

Nicola Bezzo (nicbezzo@seas.upenn.edu)
Jian Chan (jianchan@cis.upenn.edu)
Prof. Insup Lee (lee@cis.upenn.edu)
PRECISE Center
University of Pennsylvania

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation's University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

PROBLEM

V2V and V2I networks (Fig. 1) are temporary, short-duration wireless networks designed for improving the overall driving experience by exchanging a multitude of information between vehicles and fixed infrastructure. However, given the presence of malicious entities, greedy drivers, and pranksters, blindly accepting any such information received (even one received through a cryptographically secured channel) can be catastrophic. In this project, we focus on building a model for managing (computing and maintaining) the trustworthiness of messages received over V2V networks.

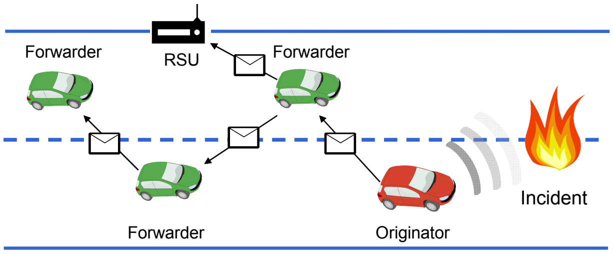
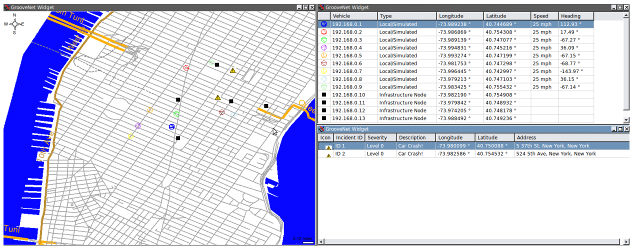


Fig.1 Example of V2V-based Incident Report

METHODOLOGY

The proposed approach takes advantage of existing V2I communication facilities deployed and managed by central traffic authorities, which can be used to collect vehicle behavior information in a crowd-sourcing fashion for constructing a more comprehensive view of vehicle trustworthiness.



	Vehicle	Type	Longitude	Latitude	Speed	Heading
○	192.168.0.1	Local/Simulated	-73.989238 °	40.744689 °	25 mph	112.93 °
○	192.168.0.2	Local/Simulated	-73.986869 °	40.754308 °	25 mph	17.49 °
○	192.168.0.3	Local/Simulated	-73.989139 °	40.747077 °	25 mph	-67.27 °
○	192.168.0.4	Local/Simulated	-73.994831 °	40.745216 °	25 mph	36.09 °
○	192.168.0.5	Local/Simulated	-73.993274 °	40.747199 °	25 mph	-67.15 °
○	192.168.0.6	Local/Simulated	-73.981753 °	40.747298 °	25 mph	-68.77 °
○	192.168.0.7	Local/Simulated	-73.996445 °	40.742997 °	25 mph	-143.97 °
○	192.168.0.8	Local/Simulated	-73.979213 °	40.747103 °	25 mph	36.15 °
○	192.168.0.9	Local/Simulated	-73.983425 °	40.755432 °	25 mph	-67.14 °
■	192.168.0.10	Infrastructure Node	-73.982190 °	40.754908 °		
■	192.168.0.11	Infrastructure Node	-73.979842 °	40.748932 °		
■	192.168.0.12	Infrastructure Node	-73.974205 °	40.748178 °		
■	192.168.0.13	Infrastructure Node	-73.988492 °	40.749236 °		

Icon	Incident ID	Severity	Description	Longitude	Latitude	Address
⚠	ID 1	Level 0	Car Crash!	-73.980099 °	40.750088 °	5 37th St, New York, New York
⚠	ID 2	Level 0	Car Crash!	-73.982586 °	40.754532 °	524 5th Ave, New York, New York

Fig.2 Screenshot of the V2V/V2I Simulator

For validating our scheme, we implemented a V2V/V2I trust simulator (Fig. 2) by extending an existing V2V simulator with trust management capabilities. Preliminary analysis of the model shows promising results. By combining our trust modeling technique with a threshold-based decision strategy, we observed on average 85% accuracy.

The trust on an endorser is computed as a triple (t, c, f). Here, t is the measured reputation value computed based on the endorser's history of providing a correct and incorrect endorsement. It could be measured as simply as (# of endorsements of factual reports/total # of endorsements) assuming independence of individual endorsements. The value c is the level of confidence on the measured reputation t, computed based on the goodness of fit of the distribution of the endorser's behavior to a specific user behavior. Finally, f is the default reputation value that is essential to reason about reports received from a vehicle that does not have any historical information available for it. The value of f is computed using static information about the endorser such as (1) vehicle make (e.g., Ford, BMW, etc.), (2) vehicle model (e.g., Corolla, Focus, etc.), (3) vehicle history (e.g., Carfax report), (4) vehicle type (e.g., ambulance, police car, etc.), (5) context information (e.g., current location: North Philly; current time: 2:00am). The vehicle uses the V2I network to obtain the static information about the endorsers, usually from the registration authority that assigns vehicle ids. Additionally, the user specifies policies to determine f, by explicitly stating its value for various combinations of static and contextual information.

As an initial step, we have designed a trust model based on Bayesian statistics. Essentially, the Bayesian trust model computes a probability estimation t by assuming the vehicle behavior can be modeled as an independent and identically distributed random variable.

RESULTS

Our simulation introduced 20 incidents with average duration 20 minutes over a map with random starting time. We assume the ground truth of the incidents are known after a five-minute delay. The start location of vehicles, the location of RSUs and incident occurrence are evenly distributed over the map area. Fig. 3 shows the trend of average trust score of vehicles with normal and attacker role types under different levels of crowd-sourced indent feedback ratio. Both the attackers and the normal vehicles begin with a trust score of 0.5. As we can see, after an initial "bootstrapping" time, the trust score of the two role types evolve in two different directions recognizing attackers from normal.

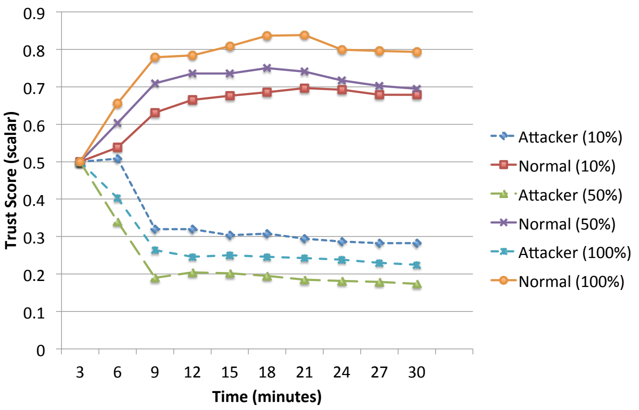


Fig.3 Average trust score trend for vehicles with attacker and normal role

CONCLUSION

By taking advantage of V2I channels between vehicles and central traffic authorities, we can construct a global view of individual vehicles trustworthiness in a crowd-sourced fashion, which overcomes the lack of vehicle behavior information due to the inherent ephemeral nature of vehicular networks. Future work is centered on improving the communication overhead, the impact of unreliable communication channel, and the cost of infrastructure deployment. Finally, we plan to further study the trade-off of security and privacy issues introduced by using unique identifiers