Poster: The ROAD to resilient location for the Internet of Vehicles

Pedro M. Rosa and Miguel L. Pardal
INESC-ID, Instituto Superior Técnico,
Universidade de Lisboa
Lisboa, Portugal
{pmgsrosa,miguel.pardal}@tecnico.ulisboa.pt

Gabriel Pestana
Faculdade Design, Tecnologia e Comunicação
Universidade Europeia
Lisboa, Portugal
gabriel.pestana@universidadeeuropeia.pt

***Abstract*—The Internet of Vehicles will allow vehicles to exchange much more information, but these interactions will require the enforcement of both safety and security policies. In this poster we adapt a widely used policy framework and propose the ROAD location subsystem to prevent GPS spoofing and other attacks. Our proposal relies on witnessing between vehicles and infrastructure, but also between passengers, bikers, and pedestrians. We argue that such redundancy and diversity will enable resilient location for future road safety.**

***Index Terms*—Connected and Autonomous Vehicles, Intelligent Transportation Systems, Location Proof Systems, Resiliency**

I. Introduction

In our work we adapt a widely used authorization framework for information systems, RFC 2904 [1], to the context of Cooperative Intelligent Transport System (C-ITS) and propose ROAD, a location subsystem that can act as a policy information point resilient to GPS spoofing and other attacks. ROAD stands for Resilient lOcation for Autonomous Driving and the name is meant to convey the core intuition of our research proposal: use everything that can be reached on the road to provide trusted location information. ROAD relies on a witnessing system of vehicles, passengers, bikers, and pedestrians, so that we have *redundancy* – many sources of information – and *diversity* – different sources of information – to achieve a resilient system. Figure 1 is a representation of the overall system where vehicles, both human-driven and autonomous, and people interact and cooperate between them, to achieve increased safety and security.

Vehicular ad-hoc networks (VANET) are evolving to Internet of Vehicles (IoV) [2]. Information sent throughout these networks can prevent collisions and help to direct traffic. However, data from several sensors in vehicles have time constraint limitations for their use, hence the need to support low *latency* communications in a moving vehicle environment.

II. Dynamic policies for Vehicles in C-ITS

Data must be secure so it can be trusted. The use of wrong information, such as awareness of self and others' location, could have serious consequences, and even cause road accidents. We propose a formal approach to safety and security, based on explicit policies. Having the safety and security rules in a policy, externalized from the vehicles, allows for evolution of that policy over time - only updates to the policy need to be redistributed. A Policy-based framework, such as AAA – Authentication, Authorization and Accounting – defined in RFC 2904 [1] and the XACML (eXtensible Access Control Markup Language), provides a standard way to document, distribute and enforce safety and security policies.

There are several stages for applying policies. They must be retrieved, evaluated and finally enforced. These actions are done in several components, abstracted as "points", called PAP, PDP, PEP and PIP. Figure 2 represents the policy framework applied to a generic C-ITS, including the management and monitoring services. The PAP is the Policy Administration Point of the policy repository, where the master copies of the policies are authored by the relevant Authorities, also represented in the Figure. The policies are distributed across the system and there are several PEP and PDP. Each Policy Enforcement Point (PEP) intercepts operations that need to be authorized, and each Policy Decision Point (PDP) interprets the policy to authorize or deny the operation. A Policy Information Point (PIP) retrieves context information and provides it to the PDP, when requested. Figure 2 shows the placement of each PIP in vehicles and in the surrounding environment. For example, in an AV, a PIP collects information from sensors to influence the current travel plan [3].

In this work we propose ROAD, Resilient lOcation for Autonomous Driving, a subsystem that acts as a location PIP, resilient to GPS spoofing and other location-based services

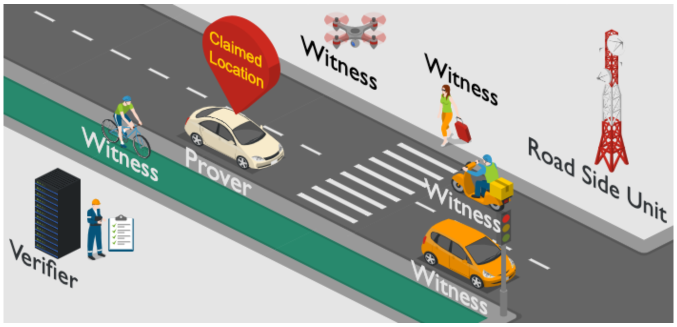

Fig. 1. Connected vehicles cooperating in road. Other devices acting as witnesses for location proofs. The proofs can be verified all these entities.

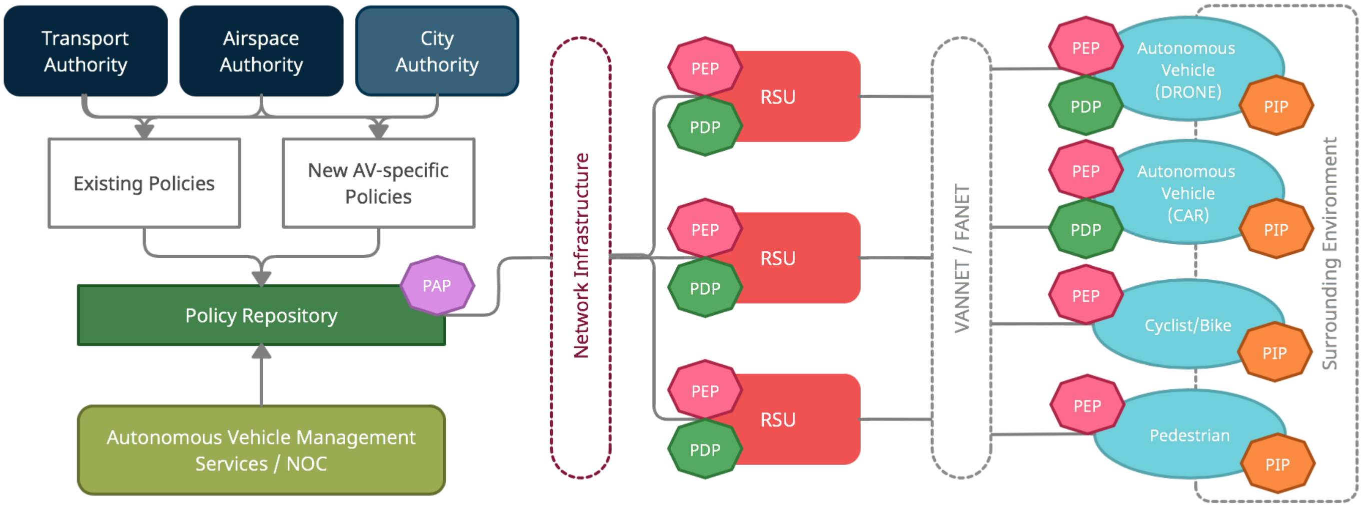

Fig. 2. Policy Framework use in Autonomous Vehicles

malfunctions. This makes acceleration, braking, and steering safer, while keeping Vulnerable Road Users (VRU) safe.

III. The ROAD to Resilient Location

The ROAD approach aims to achieve a robust and resilient location proof system for moving vehicles, providing architectural redundancy and diversity of the witness system. Resilient computing [4] defines a unified safety and security framework in the design of computer systems, and makes even more sense in services in vehicular networks and other critical cyber-physical systems. Resilience will be achieved using redundant components and plausibility checks to ensure an adversary is not tampering with the location proof system. This aims to avoid single points-of-failure and tolerate partial failures and continued compromises [5], that is, persistent and enduring problems that may eventually escalate.

Our approach will add the ability to recognize, integrate and combine proofs from different vehicle location sub-systems. Furthermore, it will integrate the different knowledge sources and resolve conflicts in a *timely* way. All the collected information will need to be processed and analyzed for plausibility reasoning, with strict response time deadlines. Overall, the approach will need to make it very difficult for an adversary, even with a synchronized attack from multiple sources, to issue false location claims for vehicles.

The ROAD architecture defines the following players: the *prover* is the vehicle that needs to prove and publish his position. The *claimed location* is the position of the prover on a given date and time, and it is very time-sensitive on moving vehicles. The *witness* is a vehicle or other actor that will share responsibility on the claimed location because it has the possibility to assure the claim is truthful. The *verifier* is another vehicle or part of the infrastructure and makes the decision to accept the claim, i.e., rely on the presented evidence and on the trusted witness(es) at the location. The interaction between these players will need decision-supporting protocols and rules: *Proof Messages*, that define messages to be exchanged between players, eventually using the ETSI ITS standard V2X messages; *Proof Plausibility Checks* to verify if the location being claimed makes sense. finally, the *Witness Verification* allows the verifier to detect the excessive reuse of witnesses and possible collusion between them and the prover.

IV. Conclusion and Future Work

A cooperative transport system needs resilient services based on secure frameworks to deliver the best results. Our proposal, ROAD, will use different players, sharing responsibilities for providing and verifying location information. The proposed framework will support a new or improved protocol for all the V2X messages, while supported on a formal security policy-based authorization framework and standard implementation language. Future work will deliver the framework design and a new PIP for supporting the resilient location services.

Acknowledgements

This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020 (INESC-ID) and through project with reference PTDC/CCI-COM/31440/2017 (SureThing).

References

[1] D. Spence, G. Gross, C. de Laat, S. Farrell, L. H. Gommans, P. R. Calhoun, M. Holdrege, B. W. de Bruijn, and J. Vollbrecht, “AAA Authorization Framework,” RFC 2904, Aug. 2000. [Online]. Available: https://rfc-editor.org/rfc/rfc2904.txt

[2] J. Contreras-Castillo, S. Zeadally, and J. Guerrero-Ibáñez, “Internet of vehicles: Architecture, protocols, and security,” *IEEE Internet of Things Journal*, vol. 5, pp. 3701–3709, 2018.

[3] G. Baldini and R. Neisse, “On the application of policy-based frameworks to autonomous vehicles,” *2020 Global Internet of Things Summit (GIoTS)*, pp. 1–6, 2020.

[4] P. Verissimo, M. Correia, N. F. Neves, and P. Sousa, “Intrusion-resilient middleware design and validation,” *Information Assurance, Security and Privacy Services*, vol. 4, pp. 615–678, 2009.

[5] A. Lima, F. Rocha, M. Völp, and P. Veríssimo, “Towards safe and secure autonomous and cooperative vehicle ecosystems,” in *CPS-SPC ’16*, 2016.