"Vehicular Steganography"?: Opportunities and Challenges

Martin Cooney, Eric Järpe, Alexey Vinel

School of Information Technology, Halmstad University, 301 18 Halmstad, Sweden
martin.daniel.cooney@gmail.com

Abstract: What if an autonomous vehicle (AV) could secretly warn of potential threats? "Steganography", the hiding of messages, is a vital way for vulnerable populations to communicate securely and get help. Here, we shine light on the concept of *vehicular steganography* (VS) using a speculative approach: We identify some key scenarios, highlighting unique challenges that arise from indirect perception, message generation, and effects of perspective–as well as potential carrier signals and message generation considerations. One observation is that, despite challenges to transmission rates and robustness, physical signals such as locomotion or sound could offer a complementary, currently-unused alternative to traditional methods. The immediate implication is that VS could help to mitigate some costly safety problems–suggesting the benefit of further discussion and ideation.

Keywords: autonomous vehicles, steganography

1 INTRODUCTION

Within the area of secure communications, this extended abstract focuses on the nascent topic of "vehicular steganography" (VS), the hiding of messages by an autonomous vehicle (AV). Conducive qualities of AVs for steganography include their many behavioral modalities, opaqueness due to high complexity, and emerging state of technological readiness that could allow for occasional odd behavior to be overlooked.

Some work has started to research VS as an extension to traditional network steganography. For example, de Fuentes et al. explored steganography in Vehicular Ad hoc Networks (VANETs) [FBGG14]. Such studies focus on methodology, but value could also emerge from identifying useful scenarios from a design perspective. Also, given the "security arms race", alternatives can be explored; although one recent study examined how an underwater vehicle could mimic animal sounds [JXF+18], studies exploring physical signals for VS appear to be rare.

To gain insight into the lay of the land, a speculative scenario-building approach was adopted, which seeks to provoke thought by constructing concrete "memories" of a potential future reality via rapid ideation and discussion sessions. This allowed us to explore the "big picture", as well as carriers, message generation strategies, and constraints for physical steganography, as in Fig. 1.[1]

[1] We expect that various other questions and scenarios also exist.

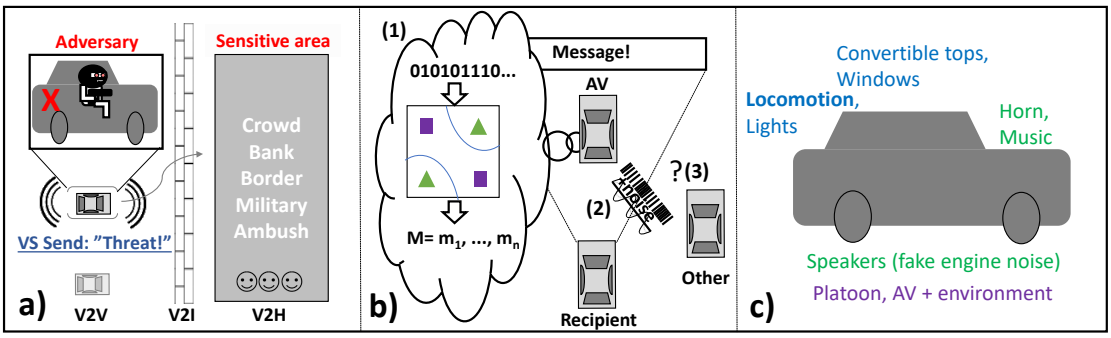

Figure 1: Basic concept: (a) motivation, (b) unique properties, (c) carriers

2 Motivation

When could an AV help humans by transmitting secret messages? Traffic safety and crime prevention appear to be crucial: Traffic accidents are the leading cause of death in young persons aged 5-29 years, involving millions of fatalities and injuries each year around the world[2], and crimes are speculated to cost trillions annually [DeL16]. Within this context, VS could deter a broad range of illicit activity: reckless or drunk driving, violent crime (hit-and-run, battery, homicide, rape), robbery and carjacking, and trafficking (drugs or humans). In the scenarios we formed, an adversary (an individual, small group, or representative of an oppressive state) displays threatening behavior while travelling inside an AV to some sensitive area such as a crowded street, bank, border, military zone, or secluded site where an ambush could take place. Indications of threat could include appearance (being armed and masked without a clear reason) or behavior (e.g. medicine non-adherence, with depression or sleep deprivation; hiding something; or potentially engaging in risky driving in manual mode, such as speeding, weaving, tailgating, and failing to yield or signal). The AV could use steganography to warn in a case where (1) the adversary might detect an unconcealed message[3] and (2) the AV is not sure about the threat and requires another opinion. These warnings could be sent to AVs or platoon members (V2V), human security (V2H), or protective infrastructure such as anti-tire spikes (V2I).

The ideation sessions also indicated some ”unique” properties of VS not evident in traditional steganography: (1) (*Generation*) No human composes the messages; the AV itself must form a message based on inference from what it has sensed. (2) (*Indirection*) In physical steganography through motion or sound, information is perceived indirectly through sensing, which could be slow and noisy. (3) (*Perspective*) Anisotropic messages could be sent to only an intended recipient at some specified angle and distance via motion or ”sound from ultrasound”, or to only young recipients via high frequency sounds.

[2] https://www.who.int/publications/i/item/9789241565684

[3] Using only encryption is not enough to hide that messages are being sent (and some public-key algorithms could also be vulnerable to quantum attacks by a technically-advanced, future adversary)

3 Carriers

In a situation where a message should be sent, steganography usually involves making small changes to little-used, redundant parts of a carrier signal (e.g. least significant bits (LSB), parity bits, or certain frequencies). Carriers are typically digital, such as network communications (communicated frames/data packets), digital text, visual media (image, video), and audio (music, speech, sounds) [ZMS14]–but AVs can also use physical carriers: Visually, motion involving varying position and orientation (paths or trajectories), velocity, or acceleration, could be used to encode messages that could be detected via communicated GPS, videos, or odometry. (Lights, and opening or closing of windows and convertible tops could also be used.) Aurally, fake engine sounds[4], or even music players or horns could be used. More complex approaches could use multimodal signals from platoons, drone swarms, the environment (e.g., like birds flying in relation to an AV's motion) or rare modalities such as heat–which modalities are used when, and how signals are amplified, ordered, or delayed, could also be considered.

4 Signal Generation

Given a carrier, codes like ASCII, Morse, or Polybius squares can be used to encode messages, but it was unclear how messages can be (1) formed and (2) embedded into a physical signal.

(1) Assuming a message comprises 1 to n short propositions m_i, of varying importance v_i (representing e.g. the nature of the emergency, location, or names) and time required to send t_i, we propose that message generation can be formulated as an unbounded Knapsack problem

$$\begin{aligned} &\max \sum v_i f(x_i) \\ \text{s. t. } T^* = &\sum t_i x_i \leq T, x_i \geq 0, \text{ and} \\ &f(2) < 2f(1) \end{aligned} \tag{1}$$

where x_i stipulates if a proposition i will be included, T is the max time available for transmission, and f is a function that rises swifty from zero then slows (e.g. $f \sim e^-(1/x)$ for $x \neq 0$, $f(0) = 0$), which expresses the higher likelihood of a proposition being received if it is repeated.[5]

(2) Assuming a simplified locomotive scenario using sideways drifting to encode Morse signals, T, the time available for sending messages can be computed by dividing d, the distance from an AV to its next interruption (e.g., an intersection) by the velocity v_0 and multiplying by α, the intended rate of message to non-message in the signal, related to encoding density (e.g. 1 : 10). Then the AV's motion could be calculated by extending a social force model, with forces relating to goal-directed motion, environmental influences, and a steganographical message. Table 1 summarizes practical constraints related to frequency, accuracy, and potential challenges.[6]

[4] https://www.core77.com/posts/79755/Cars-are-Now-So-Well-Built-Manufacturers-Pipe-In-Fake-Engine-Sounds-Listen-Here

[5] Such a formulation could be useful as Knapsack problems are greedily-solvable and have been abundantly studied, in similar combinatorial optimization contexts featuring values and costs.

[6] 1cm is our estimate based on a typical dashcam and 10m distance, and 1mm is reported for an indoors situation with markers: https://www.manufacturingtomorrow.com/article/2018/01/industrial-robots-encoders-for-tool-center-point-accuracy/10867/

Table 1: Some practical considerations for potentially useful carriers.

1 GPS	5-10Hz	5m (direct) 30-50 cm (DGPS), 2cm (RTK) [PSGU12]	How to get data (CAM)?
2 Video	30 fps	>1cm (relative), 1mm (markers)	Weather
3 Audio onset	40Hz	F_1= 0.817 [BAKS12]	Noise

5 DISCUSSION

Thus, the contribution of this paper lies in presenting some considerations for an AV to send covert messages to help people, which we refer to as *vehicular steganography* (VS). A speculative approach revealed applications to traffic safety and crime prevention; three unique qualities of VS relating to indirection, message generation, and perspective; potential carriers; initial ideas for message generation and motion steganography; and some practical constraints. Future challenges include steganalysis, perception of danger, ethics, and watermarking steganography to improve authenticity; our design process also revealed considerations for another kind of technology, socially interactive robots, which will be addressed in a separate paper, also with more technical details. By shining light on such topics, the aim is to help bring in a fresh perspective on the possibilities for AVs to create a better, safer society.

Acknowledgements: Funding was received from the Swedish Knowledge Foundation through the SafeSmart Synergy project, "Safety of Connected Intelligent Vehicles in Smart Cities".

Bibliography

[BAKS12] S. Böck, A. Arzt, F. Krebs, M. Schedl. Online real-time onset detection with recurrent neural networks. In *Proceedings of Digital Audio Effects Conference*. 2012.

[DeL16] M. DeLisi. Measuring the cost of crime. *The handbook of measurement issues in criminology and criminal justice*, pp. 416–33, 2016.

[FBGG14] J. M. de Fuentes, J. Blasco, A. I. González-Tablas, L. González-Manzano. Applying information hiding in VANETs to covertly report misbehaving vehicles. *International Journal of Distributed Sensor Networks* 10(2):120626, 2014.

[JXF+18] J. Jia-jia, W. Xian-quan, D. Fa-jie, F. Xiao, Y. Han, H. Bo. Bio-inspired steganography for secure underwater acoustic communications. *IEEE Communications Magazine* 56(10):156–162, 2018.

[PSGU12] M. Perez-Ruiz, D. C. Slaughter, C. Gliever, S. K. Upadhyaya. Tractor-based Real-time Kinematic-Global Positioning System (RTK-GPS) guidance system for geospatial mapping of row crop transplant. *Biosystems engineering* 111(1):64–71, 2012.

[ZMS14] E. Zielińska, W. Mazurczyk, K. Szczypiorski. Trends in steganography. *Communications of the ACM* 57(3):86–95, 2014.