MPC-435

January 1, 2013- December 31, 2013

**Project Title:**

Realization of a Coarse Position Verification System for an Automated Highway System

**University:**

Utah State University

**Principal Investigators:**

Ryan M. Gerdes

Assistant Professor

Dept. of Electrical and Computer Engineering

Utah State University

4120 Old Main Hill Logan, UT 84322-4120 USA

Phone: (435) 797-2840

Fax: (435) 797-3054

E-mail: ryan.gerdes@usu.edu

**Research Needs:**

To increase the throughput, efficiency, and safety of our transportation systems researchers have proposed that the system be automated and that groups of vehicles act as one unit by closely following one another at fixed speeds to form what is known as a platoon [Rajamani and Shladover, 2001]. Managing the platoon requires accurate, real-time knowledge of each vehicle’s position, velocity, and acceleration (PVA). A malicious vehicle that provides false information about its position would be able to slow down or stop the platoon, open up space for greater maneuverability, or even introduce instabilities that lead to crashes. It is therefore imperative that each vehicle’s PVA in an automated system be substantiated.

Existing methods to verify the position[[1]](#footnote-1) of an agent, of which [Capkun and Hubaux, 2006; Capkun et al., 2008; and Fiore et al., 2011] are representative, are insufficient for deployment in automated transportation as they are costly or vulnerable to attack by multiple, colluding adversaries and insiders.

**Research Objectives:**

The object for this research is to produce a technical demonstration of a technique for PVA verification that is secure regardless of the number of colluding attackers (internal or external) and can be integrated into an automated transportation system (ATS) in a cost-effective manner.

The PVA verification method that will be demonstrated operates by having vehicles respond to messages that can only be received at a given locality. Special transmitters, henceforth *waypoints*, will be designed to ensure that communication with the vehicles can only occur within a certain radius of the transmitter. The waypoints would be integrated into an ATS by placing them alongside or within the roadway, which would then allow for periodic verification of vehicle positions.

Establishing the veracity of a vehicle’s position claim using these waypoints requires a four-step process: 1) the vehicle under consideration is queried for its current location, *xa*, and velocity, *va*; 2) the distance between the alleged position and nearest upcoming waypoint, *xw*, is calculated according to *d = xw - xa*; 3) a message, consisting of a random string of binary digits known to the system, would then be transmitted at the waypoint in *d/va* seconds for the vehicle to receive; and 4) finally the vehicle would re-send the message send to the system after traveling over the waypoint to prove that it was where it said it would be. The granularity of position measurements would depend on the number and spacing of the waypoints.

The security of this approach depends upon ensuring that the verification messages could only have been received at a given locality (otherwise colluding attackers situated away from the waypoints could use antennas and amplifiers to acquire the encrypted verification message). This research will focus on the design and experimental validation of a waypoint that employs one set of antennas to transmit the verification message, with a second set placed outside the first and transmitting noise in an outward direction so as to obscure the verification message. Because of the noise a verification message is obscured and unrecoverable by an attacker situated outside the second set of antennas.

A graduate student under the PI’s supervision is currently working to extend the above verification procedure to include vehicle acceleration and establish the necessary communication protocols to facilitate verification. As the methodological component of the verification scheme is nearly complete, the purpose of research funded through this program will be to create and validate a waypoint.

**Research Methods:**

The researchers propose to use an analytical approach based on the far-field assumption to determine the appropriate type and configuration of the antennas and the requisite power requirements of the message transmitting and obscuring antennas [Stutzman and Thiele, 1998]. The researchers anticipate that existing antenna types, and hence existing analytical frameworks, will be sufficient and that no new antennas will need to be developed.

Antennas will need to be selected that are suitably small and radiate in the proper directions (e.g. the obscuring antennas should provide spherical coverage). Because the operating frequency of the antenna is related to its size and the system will have to transmit at frequencies prescribed by the Federal Communications Commission, the researchers will be constrained in their choice of antennas.

Analytical work will be verified using simulations based on either the Finite Element (FE) or Finite Difference Time-Domain methods (FDTD) [Sadiku, 2000]. The choice will depend on the operating frequency: for high operating frequencies the simpler FDTD approach becomes intractable, necessitating the use of FE. Existing commercial (e.g. COMSOL) and open source (e.g. FEMLAB) software exist for each of these approaches.

Finally, experimental work will need to be carried out ensure that the design successfully obscures the verification message at the specified distance from the waypoint. This will require the construction of a single waypoint in addition to a receiver. The researchers will assume that the communication channel can be characterized by additive white Gaussian noise (AWGN). To verify that message cannot be recovered at a certain distance, they will transmit a stream of bits and equip the receiver with a *matched filter* constructed for the bit stream. As the matched filter is an optimal detector for an AWGN channel [Couch, 2000], if the bit stream is not detected it may be concluded that the message is unrecoverable.

**Expected Outcomes:**

It is expected that this research will yield an experimentally validated waypoint design appropriate for deploying in an automated highway systems to verify a vehicle’s position claim. In addition to the waypoint prototype, the researchers further anticipate that one Master’s thesis, documenting the waypoint design and validation, will be produced as well as one journal or conference publication.

**Relevance to Strategic Goals: *Safety* and *Economic Competitiveness***

Let us assume that there are two platoons, *A* and *B*, on a freeway and that A is upstream of B. If we allow an attacker to be situated near the front of A a crash between platoons A and B could be effected in the following way. If the attacker (perhaps with external collusion) is capable of supplying false PVA information about its own location, as well as its platoons location, it could cause the vehicles behind it in A to break aggressively by making them think that the attacker's vehicle is closer than it actually is. At the same time the attacker could cause platoon B to accelerate into A by providing false information that makes B's leader believe that sufficient space exists to do so. Note that the attacker's vehicle would be unaffected in this scenario. The magnitude of the impact of the attack would depend on the speed differential of the crash that was caused by the misinformation provided to the platoons. A less severe attack would consist of B accelerating as A maintained a constant speed. This lesser attack could result in just property damage. It is apparent from the preceding how false PVA information propagating in an ATS can result in the decreased *safety* and efficiency (*economic competitiveness*) of the system.

**Educational Benefits:**

A Master’s level graduate student under the supervision of the PI will be integral to the successful completion of the project. The student will be expected to carryout analyses and simulation at the direction of the PI and, as the project progresses, to offer and execute their own design ideas. It is expected that the student will be, or quickly become, proficient in the computational electromagnetic techniques needed to carry out the simulations; an undergraduate background in antenna analysis will be required and built-upon. It is also the intention of the PI to include an undergraduate in the construction and evaluation of the prototype waypoint. The PI has found that Utah State University undergraduate students are both excited to build and work with hardware and are also competent at doing so.

**Work Plan:**

Work will begin with a review of existing antenna types to determine which are appropriate for a waypoint. Characteristics to be considered include distance to far-field, radiation pattern, radiation efficiency, and size. All of these properties will have bearing upon the final configuration of antennas. Analytical work will constitute the bulk of the analysis in this phase. A preliminary report will be filed outlining the findings of this phase, including the candidate antenna types and configuration, along with estimates of their respective power requirements. (8 months)

Having devised several candidate systems, simulation work will be undertaken in the second phase of the project to determine which system will be experimentally validated. Specifically, the distance to the far-field, radiation pattern, and radiation efficiency will estimated via simulation and compared to analytical results. An interim report will be filed that details which candidate system was chosen for experimental validation and why. (8 months)

The final task will be to confirm that the waypoint design selected in phase two does in fact obscure messages after they travel a certain distance from the waypoint. Students under the PI’s supervision will construct a prototype waypoint and then carryout the measurements and analysis necessary to demonstrate whether this has been accomplished. The validation experiments will consist of the waypoint transmitting the same message while multiple measurements made using a receiver circuit, positioned at several locations around the waypoint, are carried out. Offline analysis will then take place to see where the message could be recovered. A final report documenting the system design and experimental methodology and results will be submitted at the completion of this phase. A manuscript will be prepared for submission and the student will defend their thesis. (8 months)

**Project Cost:**

Total Project Costs: $100,000.00

MPC Funds Requested: $50,000.00

Matching Funds: $50,000 Source of Matching Funds: USU Internal

**TRB Keywords: secure localization, position verification, transportation security, autonomous vehicles, automated highway system, vehicle platooning**

**References:**

* [Capkun et al., 2008] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, “Secure location verification with hidden and mobile base stations,” Mobile Computing, IEEE Transactions on, vol. 7, pp. 470 –483, april 2008.
* [Capkun and Hubaux, 2006] S. Capkun and J.-P. Hubaux, “Secure positioning in wireless networks,” Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 221 – 232, feb. 2006.
* [Couch, 2000] L. W. Couch, Digital and Analog Communication Systems. Prentice Hall, 2000.
* [Fiore et al., 2011] M. Fiore, C. Casetti, C.-F. Chiasserini, and P. Papadimitratos, “Secure neighbor position discovery in vehicular network,” in IEEE/IFIP MedHocNet 2011, 2011.
* [Rajamani and Shladover, 2001]  R. Rajamani and S. Shladover, “An experimental comparative study of autonomous and co-operative vehicle-follower control systems,” Transportation Research Part C: Emerging Technologies, vol. 9, no. 1, pp. 15–31, 2001.
* [Sadiku, 2000] M. N. O. Sadiku, Numerical Techniques in Electromagnetics. CRC Press, 2000.
* [Stutzman and Thiele, 1998] W. L. Stutzman and G. A. Thiele, Antenna Theory and Design. Wiley, 1998.

1. The velocity of a vehicle can be computed by finding the entity’s position at two instances in time and dividing by the time difference; acceleration is calculated in a similar manner but by using two velocity measurements. As velocity and acceleration are derivable from position, only secure positioning methods need be considered to obtain velocity and acceleration in a secure manner. [↑](#footnote-ref-1)