VANET Privacy

SVSU FACULTY RESEARCH GRANT PROPOSAL

George Corser
November 15, 2014

ABSTRACT

The US Department of Transportation will mandate a new vehicle safety system, the vehicle network. Just as vehicles now have seatbelts and airbags, all cars, trucks and other vehicles in the future will be required to contain wireless network routers. These are similar to wi-fi devices found in coffee shops and residential homes, except built on a different technical architecture which allows them to function while in motion at vehicle speeds. This new network, the vehicular ad hoc network, or VANET, may one day save thousands of lives and billions of dollars, reduce fuel consumption and pollution, and expand ubiquitous connectivity and mobile application functionality to the world's roadways. Problem: VANETs may violate drivers' privacy, exposing motorists to surveillance by eavesdroppers, from casual stalkers to Big Brother. Existing location privacy research has not thoroughly considered vehicular mobility patterns and unique architectures.

Research goals, methods, and anticipated outcomes: The proposed research would evaluate and develop new privacy models using realistic vehicle mobility patterns. New and existing vehicular privacy protocols would be tested using computer simulation tools. The expected contribution is a formalization and quantification of the relationship between safety/security, network/application service quality/efficiency, and privacy.

NARRATIVE

The vehicular ad-hoc network (VANET), sometimes called "The Internet of Cars," presents distinctive location privacy challenges. In the United States VANET standards are specified by Dedicated Short Range Communications / Wireless Access in Vehicular Environments (DSRC/WAVE). These standards call for media access control layer (MAC layer) transmissions of precise vehicle locations 10 times per second. DSRC can be used to access the Internet, including LBS applications which may also require frequent precise location (FPL) data.

The location privacy challenge from a technical standpoint is large-scale and complicated in VANETs. Equipment supporting wireless/wifi networks is already being installed in new vehicles. Industry representatives estimate that 90% of vehicles will be wifi-connected within the decade [1]. LBS usage continues to grow rapidly [2] and is expected to expand to VANET platforms [3]. Standards governing VANETs [4] provide data fields for future privacy protocols, but the specifics of these protocols remain open research questions.

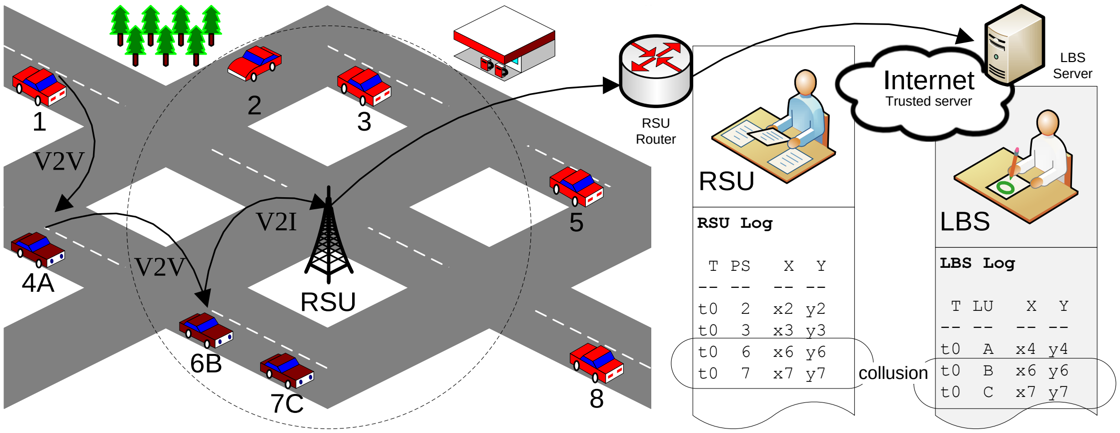
The literature refers to several forms of privacy. *Identity privacy* is sometimes referred to as anonymity, pseudonymity or unlinkability with personally identifiable information (PII). This is often achieved by the use of pseudonyms. *Location privacy* refers to the unlinkability of PII with a geographical position, and further, the unlinkability of one pseudonym with another by using location data. *Query privacy* would make unlinkable to the user's PII, not only the location of the user, but also the particular query made or query service used. Privacy must be constrainable, as in the cases of *conditional privacy* and *revocability*. This research would focus on location privacy.

1. **Goals and Objectives**

This research would address the two primary vehicular network location privacy questions**:** To what extent can a vehicle protect itself against surveillance even while using a location based service (LBS), which may require frequent hyper-accurate location data? And what are the cost/benefit tradeoffs?

2. **Background and Context**

Location privacy attackers could range from casual stalkers to Big Brother. Vehicles in VANETs can communicate vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I). When contacting LBS vehicles communicate V2I through a wireless access point called a roadside unit (RSU). Figure 2 shows how vehicles may communicate with LBS via multi-hop V2V. The present research excludes other forms of communication, such as cellular and WiMax.



RSU Log

T	PS	X	Y
t0	2	x2	y2
t0	3	x3	y3
t0	6	x6	y6
t0	7	x7	y7

LBS Log

T	LU	X	Y
t0	A	x4	y4
t0	B	x6	y6
t0	C	x7	y7

Figure 1: Network Model and Threat Model

Powerful RSU system administrators may have access to one, many or all RSUs. If LBS administrators have access to RSU data, LBS and RSU location data could be cross-referenced, as shown in Figure 1.

3. **Significance and Impact**

Special qualifications: I have published several papers [5] [6] [7] and I am awaiting the publication of my dissertation and two more papers in this research area. I have written and spoken on this topic at scholarly conferences and other venues nationwide.

Significance/impact to my research work: Someday, someone will discover a privacy protocol that widely applies in vehicular networks. I hope that someone will be me. The proposed project will build on my prior research work, so it will certainly accelerate my primary research.

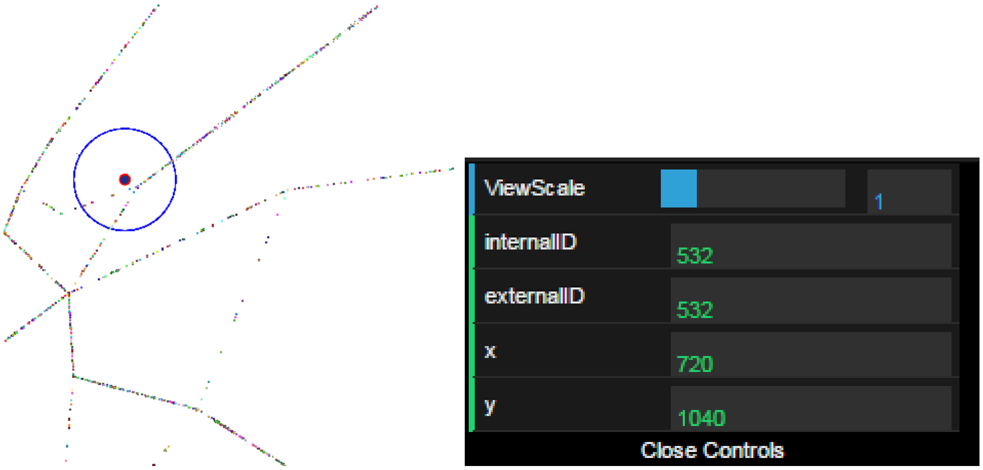
Significance/impact to my discipline: My discipline is vehicle network security, which generally covers the confidentiality, integrity and availability of vehicle network communications. Digital privacy is one of the great information challenges of our time, and preserving privacy in vehicular network is one of the great open research challenges in the field of vehicle network security. If new relationships could be identified, or if a simulation architecture could be established and widely accepted by researchers, then advancements may be forthcoming which might apply even outside the field of vehicular network security.

Significance/impact to SVSU: SVSU is located in Michigan, the heart of the automotive manufacturing industry. If SVSU were to expand research in cutting edge automotive research fields, SVSU may open new avenues for relationships with local industry.

Significance/impact to society in general: The vehicular location privacy problem is important to society because driver location data can be misused. Employers might monitor an employee's car parked at a competitor's office (revealing an employee's job interview) or at specialized medical facilities (revealing an employee's health condition). It is not difficult to construct further privacy breaches arising from vehicle surveillance by spouses and ex-spouses, or paparazzi and other stalkers. Proposed national level legislation in the United States to address digital location privacy threats includes the Location Privacy Act and the Geolocation Privacy and Surveillance Act. Without privacy protections in place, wireless eavesdroppers or malicious LBS administrators could track specific vehicles, or cross-reference vehicles' precise origin and termination geographical coordinates with home and work addresses, using Google Maps or some similar map database, perhaps revealing (*deanonymizing*) a vehicle at a given location at a given time. Because motor vehicles tend to move at high speeds in predictable patterns along prescribed routes, their mobility patterns may make vehicles more vulnerable to location privacy attacks than, say, pedestrian mobile phone users. Deanonymization could occur at either the MAC layer or higher layers. MAC layer VANET systems require vehicles to transmit FPL. LBS applications sometimes have similar requirements. If there is collusion, MAC layer data could be used to circumvent application layer (APP layer) protections such as spatial-temporal cloaking. Legal solutions are only partly effective. A technical solution is indicated.

4. **Methods/Procedures/Materials**

In order to test location privacy models, it is necessary to position vehicles at various locations in a road network and determine how long they are in communications range. It is cost prohibitive to purchase a real-world road network, complete with real drivers and real cars equipped with real VANET routers. So research uses computer simulations.



ViewScale 1
internalID 532
externalID 532
x 720
y 1040

Figure 2: Visutrace Visualizer built at SVSU

Method: I have developed my own software to simulate vehicle locations. I have also led the development of new tools here at SVSU. Figure 2 shows a tool designed by me and coded by SVSU undergraduate Dustyn Tubbs as part of his work in a class I am teaching, CIS 255. See: Visutrace Visualizer: www.svsu.edu/~djtubbs1/cis255.

The general plan of work for this project is to systematically simulate new and existing privacy models against new and existing vehicular mobility patterns. I have established a testbed for one privacy model (the null model, i.e. no privacy) against City, Urban and Rural mobility patterns in Zurich. Let’s name these Privacy Model / Mobility Pattern (PM/MP) simulations as follows.

- Null / City, Null / Urban, and Null / Rural.

Procedure: The next step will be to add models and mobility patterns. New privacy models would include RRVT, EPZ and PBD. New mobility patterns could include Manhattan, Freeway, Roundabout, Gas Station. So new PM/MP simulations would include

- RRVT / City, RRVT / Urban, RRVT / Rural, RRVT / Manhattan, RRVT / Freeway, RRVT / Roundabout, RRVT / Gas Station
- EPZ / City, EPZ / Urban, EPZ / Rural, EPZ / Manhattan, EPZ / Freeway, EPZ / Roundabout, EPZ / Gas Station
- PBD / City, PBD / Urban, PBD / Rural, PBD / Manhattan, PBD / Freeway, PBD / Roundabout, PBD / Gas Station

For each PM/MP simulation, the student will follow these steps.

- Step 1: Code privacy model into software.
- Step 2: Generate mobility pattern and load into simulation environment.
- Step 3: Run simulation. This can take several days even on a fast computer.
- Step 4: Record, write-up results.

In the future I hope to engage vehicle network privacy researchers worldwide to try their models and mobility patterns on my platform.

Materials: The project requires one or more computers that can be dedicated to running simulations for days or even weeks at a time.

5. **Timeline**

July 2015	– Prep simulation environment
August	– Student runs experiment #1
September	– Prof and student write-up conference paper
October	– Student runs experiment #2
November	– Prof and student write-up conference paper
December	– Break
January 2016	– Student runs experiment #3
February	– Prof and student write-up journal paper
March	– Student runs experiment #4
April	– Prof and student write-up journal paper
May	– Break
June	– Prof writes final report

6. **Contingency or alternate plans.**

Contingency #1: Equipment fails. If this happens I can run simulations on my office desktop, but that will slow down everything else I do.

Contingency #2: Student resigns from job. If this happens I have backup people identified. Since I can complete all tasks myself, even if no student can be identified I can do the work but it will take more calendar time. I would likely apply for an extension in this case.

7. **Evaluation:**

Findings will be published in one of the relevant conference proceedings and/or journals. Specific targets: Vehicular Technology Conference (VTC), IEEE Transactions on Vehicular Technology (TVT), International Conference on Connected Vehicles & Expo (ICCVE), IEEE Intelligent Vehicles Symposium (IV).

I will know that the project is making progress in meeting the goals because a checklist will be posted in my office and on my website. Progress can be monitored by all relevant parties. The checklist will look something like this.

Table 1: Project Checklist

Privacy	Mobility						
Model	Model	AS	E(AS)	PT	SD	LD	DST
Null	City						
Null	Urban						
Null	Rural						
Null	Manhattan						
Null	Freeway						
Null	Roundabout						
Null	Gas Station						
RRVT	City						
RRVT	Urban						
RRVT	Rural						
RRVT	Manhattan						
RRVT	Freeway						
RRVT	Roundabout						
RRVT	Gas Station						
EPZ	City						
EPZ	Urban						
EPZ	Rural						
EPZ	Manhattan						
EPZ	Freeway						
EPZ	Roundabout						
EPZ	Gas Station						
PBD	City						
PBD	Urban						
PBD	Rural						
PBD	Manhattan						
PBD	Freeway						
PBD	Roundabout						
PBD	Gas Station						

BUDGET

To summarize, the overall project budget is as follows.

$2500	Student assistant
$1000	Simulation Workstation (Computer)
$1500	Conference fees/travel
$5000	TOTAL

- Release time is required for Winter 2016 because this project will yield a journal paper. Journal papers are time-consuming to write. In order to maximize the chances of acceptance the time investment is required.

- Student wages are estimated to be $2400 in total, which represents 240 hours at $10 per hour. See below.

Table 2: Budget Detail for Student Assistant

Date	Activity	Stud-Hrs	Stud-Rate	Stud-Cost	Cum-SC
7/1/2015	Prep simulation envt	4	$ 10.00	$ 40.00	$ 40.00
7/8/2015	Prep simulation envt	4	$ 10.00	$ 40.00	$ 80.00
7/15/2015	Prep simulation envt	4	$ 10.00	$ 40.00	$ 120.00
7/22/2015	Prep simulation envt	4	$ 10.00	$ 40.00	$ 160.00
7/29/2015			$ 10.00	$ -	$ 160.00
8/5/2015	Student runs EXP1	10	$ 10.00	$ 100.00	$ 260.00
8/12/2015	Student runs EXP1	10	$ 10.00	$ 100.00	$ 360.00
8/19/2015	Student runs EXP1	10	$ 10.00	$ 100.00	$ 460.00
8/26/2015	Student runs EXP1	10	$ 10.00	$ 100.00	$ 560.00
9/2/2015	Write-up EXP1	4	$ 10.00	$ 40.00	$ 600.00
9/9/2015	Write-up EXP1	4	$ 10.00	$ 40.00	$ 640.00
9/16/2015	Write-up EXP1	4	$ 10.00	$ 40.00	$ 680.00
9/23/2015	Write-up EXP1	4	$ 10.00	$ 40.00	$ 720.00
9/30/2015			$ 10.00	$ -	$ 720.00
10/7/2015			$ 10.00	$ -	$ 720.00
10/14/2015	Student runs EXP2	10	$ 10.00	$ 100.00	$ 820.00
10/21/2015	Student runs EXP2	10	$ 10.00	$ 100.00	$ 920.00
10/28/2015	Student runs EXP2	10	$ 10.00	$ 100.00	$ 1,020.00
11/4/2015	Student runs EXP2	10	$ 10.00	$ 100.00	$ 1,120.00
11/11/2015	Write-up EXP2	4	$ 10.00	$ 40.00	$ 1,160.00
11/18/2015	Write-up EXP2	4	$ 10.00	$ 40.00	$ 1,200.00
11/25/2015	Write-up EXP2	4	$ 10.00	$ 40.00	$ 1,240.00
12/2/2015	Write-up EXP2	4	$ 10.00	$ 40.00	$ 1,280.00
12/9/2015	Submit for publication		$ 10.00	$ -	$ 1,280.00
12/16/2015			$ 10.00	$ -	$ 1,280.00
12/23/2015			$ 10.00	$ -	$ 1,280.00
12/30/2015			$ 10.00	$ -	$ 1,280.00
1/6/2016	Student runs EXP3	10	$ 10.00	$ 100.00	$ 1,380.00
1/13/2016	Student runs EXP3	10	$ 10.00	$ 100.00	$ 1,480.00
1/20/2016	Student runs EXP3	10	$ 10.00	$ 100.00	$ 1,580.00
1/27/2016	Student runs EXP3	10	$ 10.00	$ 100.00	$ 1,680.00
2/3/2016	Write-up EXP3	4	$ 10.00	$ 40.00	$ 1,720.00
2/10/2016	Write-up EXP3	4	$ 10.00	$ 40.00	$ 1,760.00
2/17/2016	Write-up EXP3	4	$ 10.00	$ 40.00	$ 1,800.00
2/24/2016	Write-up EXP3	4	$ 10.00	$ 40.00	$ 1,840.00
3/2/2016			$ 10.00	$ -	$ 1,840.00
3/9/2016			$ 10.00	$ -	$ 1,840.00
3/16/2016	Student runs EXP4	10	$ 10.00	$ 100.00	$ 1,940.00
3/23/2016	Student runs EXP4	10	$ 10.00	$ 100.00	$ 2,040.00
3/30/2016	Student runs EXP4	10	$ 10.00	$ 100.00	$ 2,140.00
4/6/2016	Student runs EXP4	10	$ 10.00	$ 100.00	$ 2,240.00
4/13/2016	Write-up EXP4	4	$ 10.00	$ 40.00	$ 2,280.00
4/20/2016	Write-up EXP4	4	$ 10.00	$ 40.00	$ 2,320.00
4/27/2016	Write-up EXP4	4	$ 10.00	$ 40.00	$ 2,360.00
5/4/2016	Write-up EXP4	4	$ 10.00	$ 40.00	$ 2,400.00
5/11/2016	Submit for publication		$ 10.00	$ -	$ 2,400.00
5/18/2016			$ 10.00	$ -	$ 2,400.00
5/25/2016			$ 10.00	$ -	$ 2,400.00
6/1/2016	Prof writes final report		$ 10.00	$ -	$ 2,400.00
6/8/2016	Prof writes final report		$ 10.00	$ -	$ 2,400.00
6/15/2016	Prof writes final report		$ 10.00	$ -	$ 2,400.00
6/22/2016	Prof writes final report		$ 10.00	$ -	$ 2,400.00
6/29/2016	Prof submits final report		$ 10.00	$ -	$ 2,400.00

- Equipment: Computer simulations require a computer. Prices fluctuate, but even today fast i7-processor desktops are available for under $1000. See Lenovo ThinkCenter ($919.99) (link)

- Supplies and materials: none.

- Travel costs: In order to build future research on the most up-to-date current research, it is necessary to mingle with the world's top researchers. The most appropriate venue is the VTC. The 2015 conference will be held in Boston in September.

- Other Costs: none

CURRICULUM VITAE

CV appears at end of this document.

PREVIOUS FUNDING SUPPORT & PROGRESS REPORTS

None

REFERENCES

[1] Bush, I. (2013, Feb 25). GM, AT&T readying in-vehicle wi-fi. http://philadelphia.cbslocal.com/2013/02/25/gm-att-readying-in-vehicle-wi-fi/

[2] Johnson, L. (2012, Oct 31). Location-based services to bring in $4b revenue in 2012: study. http://www.mobilemarketer.com/cms/news/research/14115.htmlhttp://www.mobilemarketer.com/cms/news/research/14115.html

[3] Koslowski, T. (2012, Jan 3). Your connected vehicle is arriving. http://www.technologyreview.com/news/426523/your-connected-vehicle-is-arriving/

[4] IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006) , vol., no., pp.1,289, April 26 2013, doi: 10.1109/IEEESTD.2013.6509896

[5] Corser, G., Fu, H., Shu, T. D'Errico, P., Ma, W. (2013, December). Endpoint Protection Zone (EPZ): Protecting LBS user location privacy against deanonymization and collusion in vehicular networks. In Second International Conference on Connected Vehicles & Expo. IEEE.

[6] Corser, G., Fu, H., Shu, T. D'Errico, P., Ma, W., Leng, S., Zhu, Y. (2014, June). Privacy-by-Decoy: Protecting Location Privacy Against Collusion and Deanonymization in Vehicular Location Based Services. In 2014 IEEE Intelligent Vehicles Symposium. IEEE. Dearborn, MI.

[7] Alnahash, N., Corser, G., Fu, H. (2014, April). Protecting Vehicle Privacy using Dummy Events. In 2014 American Society For Engineering Education North Central Section Conference (ASEE NCS 2014).

CURRICULUM VITAE

George Corser

PhD Dissertation Topic

Protecting location privacy in vehicle networks, especially within location based service (LBS) applications, is the focus of my dissertation. This involves defining privacy in computational terms, establishing measurement metrics, identifying vulnerabilities peculiar to the vehicular network environment and simulating protocols that would protect vehicle location privacy. My own method, privacy-by-decoy, would protect users of location based services by establishing transmission silence near home and office endpoints, and by relaying decoy requests through vehicles of non-users.

Vehicle Network Related Publications, as First Author

- Corser, G., Fu, H., Shu, T. D'Errico, P., Ma, W., Leng, S., Zhu, Y. (2014, June). Privacy-by-Decoy: Protecting Location Privacy Against Collusion and Deanonymization in Vehicular Location Based Services. In *2014 IEEE Intelligent Vehicles Symposium*. IEEE. Dearborn, MI.
- Corser, G., Fu, H., Shu, T. D'Errico, P., Ma, W. (2013, December). Endpoint Protection Zone (EPZ): Protecting LBS user location privacy against deanonymization and collusion in vehicular networks. In *Second International Conference on Connected Vehicles & Expo*. IEEE. Las Vegas, NV.

Vehicle Network Related Publications, as Second Author

- Alrajei, N., Corser, G., Fu, H., Zhu, Y. (2014, February). Energy Prediction Based Intrusion Detection In Wireless Sensor Networks. International Journal of Emerging Technology and Advanced Engineering (IJETAE), Volume 4, Issue 2. (**Journal**)
- Oluoch, J., Corser, G., Fu, H., Zhu, Y. (2014, April). Simulation Evaluation of Existing Trust Models in Vehicular Ad Hoc Networks. In 2014 American Society For Engineering Education North Central Section Conference (ASEE NCS 2014).
- Alnahash, N., Corser, G., Fu, H. (2014, April). Protecting Vehicle Privacy using Dummy Events. In 2014 American Society For Engineering Education North Central Section Conference (ASEE NCS 2014).

Education

Oakland University, Rochester, Michigan (Pending: expected July, 2014)
* **PhD—Computer Science and Informatics** (*ABD: all but dissertation)

- Dissertation topic: Securing location privacy in vehicular communications systems and applications

University of Michigan–Flint, Flint, Michigan (Received: August 2011)
MS, Computer and Information Science (CAIS)

- King-Chavez-Parks Future Faculty Fellowship 2009-10

Princeton University, Princeton, New Jersey (Received: June 1985)
BSE, Civil Engineering

- Undergraduate thesis: Closed-end Funds and Securities Market Efficiency

Employment

Saginaw Valley State University, Saginaw, Michigan (July 2014 to present)
Assistant Professor

- Computer Science and Information Systems (CSIS) Department
- Teaching CS 116 (Introduction to Programming I, Linux/C++)
- Teaching CIS 255 (Client Side Web Development, HTML, CSS, JavaScript)
- Teaching CIS 355 (Server Side Web Development, PHP, MySQL)

Oakland University, Rochester, Michigan (July 2011 to May 2014)
Instructor and Teaching Assistant (part time, concurrent with full time PhD studies)

- Instructor: Taught CRJ 341, Cybercrime, as Instructor, in Criminal Justice department, Winter 2014.
- Instructor: Taught one undergraduate course, CIT 448, Information Security Practice, as Instructor, in Computer Science and Engineering department, Fall 2012. Received 90% student approval rating (4.5/5.0).
- Teaching Assistant: Informally assisted with CIT 247, Introduction to Computer Networks, and CSE 647, Advanced Computer Networks, lecturing occasionally. Served as teaching assistant in six (6) other undergraduate courses, lecturing occasionally. Also lectured in graduate courses, CSE 681, Information Security, and CSE 647, Advanced Computer Networks. Created YouTube channel, OaklandCSE, for computer science education. Channel has 100+ videos, 200+ subscribers and 50,000+ views.
- Grants and Proposals: Helped prepare NSF grant documents. Currently helping prepare proposal materials for new program for master's degree in cybersecurity. Helped deliver on NSF grant, Research Experience for Undergraduates (REU).

ITT Tech, Troy, Michigan (June 2011 to August 2012)
Adjunct Instructor (part time, concurrent with Oakland University, above)

- Taught seven (7) undergraduate level computer courses as Instructor. Received outstanding student evaluations.

University of Michigan–Flint, Flint, Michigan (September 20 to December 2010)
Graduate Student Research Assistant (part time, while full time Masters student)

- Researched and reported academic advancements in the field of computer ethics.

Vehicle Network Related Association Memberships

- IEEE Vehicular Technology Society, MEMBER (Since 2013)