Southeastern Transportation Center
Proposal Cover Page
O/E Grant 2016-2017

UNIVERSITY:	Clemson University		
TITLE OF PROJECT:	Development of a Security Platform for Vehicle to Infrastructure Network		
FEDERAL FUNDS:			
Requested Amount	**Proposed Duration:**		**Desired Start Date:**
$ 49,850	12 months		May 02, 2016
MATCHING FUNDS:			
Source 1: University Funds		**Source 2:**	
$ 49,850		$	
DEPARTMENT SUBMITTING PROPOSAL:			
PI Name/Title: Mashrur (Ronnie) Chowdhury, Mays Endowed Professor of Transportation			
Address: 218 Lowry Hall, Clemson, SC 29634			
Phone: 864-656- 3313			
Fax: 864-656-2670			
Email: mac@clemson.edu			
Signature: Mashrur Chowdhury			**Date:** 2/11/16
SUBCONTRACTING INSTITUTION:			
ADMINISTRATIVE REPRESENTATIVE AUTHORIZED TO CONDUCT NEGOTIATIONS:			
Name/Title: Tanju Karanfil, Vice President for Research			
Address: 300 Brackett Hall, Clemson, SC 29634-5701			
Phone: 864-656-7701			
Fax: 864-656-7700			
Email: tkaranf@clemson.edu			
Signature:			**Date:** 2/12/16
ADMINISTRATIVE ORGANIZATION'S REPRESENTATIVE:			
Name/Title: Dianne Myers			
Address: 113 Riggs hall, Clemson, SC 29634			
Phone: 864-656-5534			
Fax: 864-656-4518			
Email: dmmyers@clemson.edu			
Signature:			**Date:** 2/12/16
OTHER REQUIRED SIGNATURES:			
Name/Title:			
Address:			
Phone:			
Fax:			
Email:			
Signature:			**Date:**

SIGNATURE

2. Problem Statement

The driving force behind the US economic engine is the surface transportation system in that it enables reliable and efficient transportation of passengers and goods. Despite the remarkable improvement in vehicle design and performance that has improved vehicle safety, more than 30,000 fatalities occur on US highways annually [1]. Unfortunately, human error is the leading cause of these fatalities, and cannot be solved through the mechanical design of the vehicle [2]. To reduce the large number of fatalities and associated societal costs, the US Department of Transportation (USDOT) has been promoting connectivity between vehicles (known as vehicle to vehicle or V2V) and between vehicles and intelligent transportation infrastructure (known as vehicle to infrastructure or V2I), enabled by wireless communication technology (e.g., dedicated short-range communication or DSRC). V2V and V2I technologies provide vehicles with a 360 degree of awareness, which will support safety (such as collision warning), mobility (such as queue warning) and environmental (such as connected eco driving) applications [3]. USDOT has been piloting these technologies in a limited scale at several pilot deployment sites around the US. One of the major challenges inherent in these deployments involves the real-time secure processing and distribution of the massive amounts of data generated by connected vehicles and roadside equipment to provide safety, mobility and environmental-related services to travelers.

Ensuring that the connected transportation ecosystem is cognizant of potential cyber-attacks is of the utmost importance. Specifically, ensuring the secure communication between diverse stakeholders in connected transportation systems is perhaps the major challenge to a safe and reliable operation of such system. In the era of Internet of Things (IoT), security challenges are dynamic, and the constant detection of potential threat and development of appropriate/effective countermeasures are of paramount importance. The primary security risks could be originated in different interface levels in connected transportation systems, such as V2V, V2I or Infrastructure to Infrastructure (I2I). For example, a traffic signal that communicates with a vehicle in supporting different safety, mobility and environmental applications must participate in the network security. There is also the question of public agency involvement in governance of the secure communication network, which is a relevant technical issue, as it implies a developing and maintaining of a communication platform with roadside equipment and security certificates. The network security in general is the biggest hurdle. Transportation agencies must design and build a secure ecosystem that can detect and eliminate potential threats to the connected vehicle (CV) environment.

However, today's Information Technology (IT) security ecosystem, which relies on a combination of static perimeter network defenses (e.g., firewalls and intrusion detection/prevention systems), ubiquitous use of end-host based defenses (e.g, antivirus), and software patches from vendors (e.g., Patch Tuesday), is fundamentally ill-equipped to handle the security issues in the connected vehicle ecosystem. In this research, we propose to build a flexible and reliable security protection mechanism for a CV ecosystem, leveraging emerging network techniques. We will model diverse security risk scenarios in a V2I communication environment that will provide a much-needed guidance to establish a secure and resilient communication for future connected vehicle technology deployments in the real world. The

proposed project will perform field evaluations of our proposed security protection mechanisms in real-world environments in the city of Clemson, South Carolina.

3. Research Objective

The objectives of this research are as follows:

- Develop a V2I security platform for cyber-attack capturing, analysis and countermeasure Implementation, and
- Perform field tests to evaluate the performance of security solutions enabled by our security platform in the V2I interfaces.

4. Research Approach

This research focuses on the identification and analysis of V2I interfaces for the purpose of developing security controls that afford the right level of protection given the data and means of transmission. Traditional static perimeter defenses are unable to secure CVs, since these vehicles are deployed deep inside the network with a constant mobility. To enforce security policies based on the dynamic context, we envision a new *software-defined approach to secure V2I interfaces in* CV ecosystem with the proposed development of a security platform for the V2I network, where we can: (a) rapidly develop and deploy novel network defenses tailored to various security requirements in a CV ecosystem, and (b) dynamically customize the network's security posture to the current operating context of different vehicles and the surrounding roadway environment.

Figure 1 shows a high-level vision of CV V2I security architecture called CVGuard, which envisions customized µmboxes (includes micro network-security functions in a cloud) that act as (1) security gateways for each vehicle and (2) a dynamic attack capturing and analysis platform for V2I interfaces. A logically centralized CVGuard controller (resides in the cloud as well) monitors the contexts of different vehicles and V2I communications, identifies and analyzes security threats, and implements solutions to the threats.

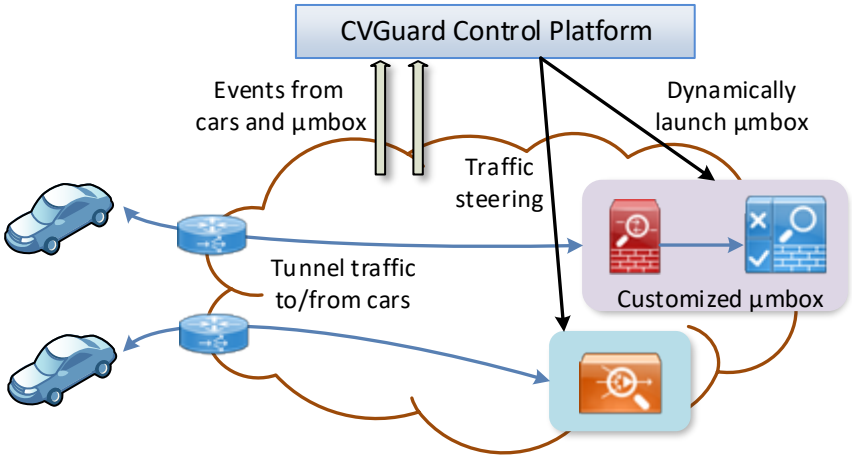

Figure1. CVGuard: Connected Vehicle V2I Security Architecture

CVGuard will support three types of network security functions: (i) attack prevention functions (e.g. firewalls and Intrusion Prevention System or IPS); (ii) attack detection functions (e.g. Intrusion Detection System (IDS), scan and Distributed Denial of Service (DDoS) detector);

and (iii) attack capturing functions (e.g. honeypot). In particular, CVGuard provides a centralized security function controller to enable dynamic interoperation and automatic reconfiguration of security functions. IDSs can then reconfigure their detectors based on the new or updated attack patterns. When IDSs detect malicious behaviors, they can either redirect malicious data traffic to attack capturing appliances for further monitor or notify firewalls to update their configuration and block network traffic. In addition, for the automate detection and mitigation of attacks in V2I interfaces, CVGuard provides a rapid response to threats, with the ability to rapidly steer or quarantine data flows based on real-time network conditions. The primary goal of CVGuard is to detect and isolate any cyber-attack in a V2I environment before they can negatively affect vehicles or transportation networks, which could lead to crashes and hamper the adoption of connected vehicle technology. Upon discovering a potential threat, CVGuard identifies the problem and automatically adopts the necessary resolution strategies. After containing the threat, CVGuard automatically allows the V2I components to rejoin the network. The specific tasks we will pursue in this project are illustrated in Figure 2 and discussed in the following subsections:

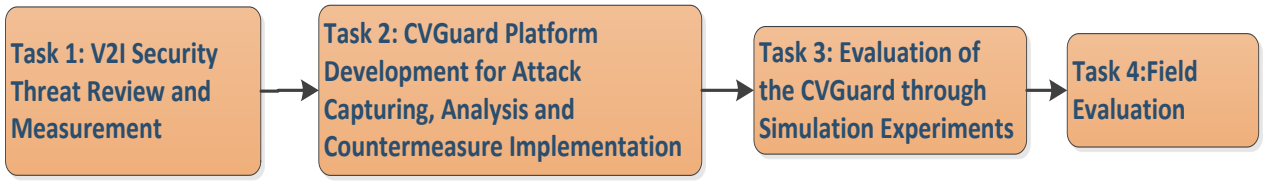

Figure 2: Research Tasks

Task 1: V2I Security Threat Review and Measurement

There are number of existing research efforts on addressing security threats against CV environments. In this task, we will first review those research efforts and identify *unique* security challenges and measure security risks for those threats specifically targeting a V2I environment. We will then develop different use cases of cyber-attack scenarios, which include the integrity attack, false data injection (or deception attack), and denial of service (DoS), in the V2I environment. In addition, we will identify security risks of those specific threats for V2I communication interfaces by reviewing the National Vulnerability Database (NVD) [4]. The MITRE CVE (Common Vulnerabilities and Exposures) database will be used to identify the vulnerabilities that could be exploited by remote control attacks. We will use the Common Vulnerability Scoring System (CVSS) matrix developed by the NVD to prioritize the damage potential of different vulnerabilities and associated exploitability in a V2I environment. The probability of a successful attack will be determined by calculating probability of exploitability of the vulnerabilities by estimating the CVSS score.

Task 2: CVGuard Platform Development for Attack Capturing, Analysis and Countermeasure Implementation

In this task, we will develop a CVGuard platform using the emerging Software Defined Network (SDN) technique [5] that will centrally analyze various data obtained from the CVs through a V2I network to learn new attackers' patterns and/or behaviors and to adaptively response to the attackers. The security analyzer is one of the key strategic approaches for measuring and evaluating the severity of identified security vulnerability or breaches related to

attack vectors identified in Task 1. After receiving an indicator from CVGuard, the alert analyzer matches the alert in an Attack Correlation Graph (ACG) [6] to correlate attackers' behaviors. For example, if the alert already exists in the graph and is a known attack (i.e., matching the attack signature) the security analyzer performs a countermeasure selection procedure based on both positive impact, such as countermeasure effectiveness, and negative impact, such as deployment cost and intrusiveness to existing applications. CVGuard then notifies the SDN network controller or software controller to deploy countermeasures or mitigation actions. If the alert is new, the security analyzer will perform alert correlation, and analysis and update the Scenario Attack Graph (SAG). CVGuard will apply selected countermeasure according to the severity of the security evaluation results. This approach is quite innovative in that it appropriately decides when to apply the countermeasures.

Task 3: Evaluation of the CVGuard through Simulation Experiments

We will evaluate CVGuard in a virtual network using the Network Simulator Version 3 (ns-3), a high fidelity communication network simulator, extensively used in computer networking research and development [7]. We will first simulate cyber-attack scenarios from the attackers' perspective with maximum damage potentials to connected transportation system V2I interface level, which we can further exploit in V2V or I2I interfaces (note: determining the V2V and I2I interface security is not the focus of this research). We will next evaluate the performance and effectiveness of the CVGuard in capturing and analyzing the attack for purposes of identifying appropriate countermeasures against the threats to neutralize the attack. In a hierarchal level, if any counter-measure fails, the attack moves to next level and keeps assuming control of the system components in different levels. We will use throughput, message delay and packet loss to evaluate the performance of CVGuard, and leverage various attack scenarios to evaluate the effectiveness of CVGuard.

Task 4: Field Evaluation

Unlike the previous task in which we simulated the threats and their impacts in a virtual environment, here we will develop and implement threat models representing various types of deliberate, real-world attacks on test CVs and roadside units. The research team will utilize the V2I connected vehicle technology resource (e.g., the DSRC vehicle on-board units and roadside units) available at the Connected Vehicle Research Laboratory directed by Dr. Chowdhury, the proposed PI, for our field evaluation of the CVGuard security solutions. The research team also has Connected Vehicle Communication infrastructure that support heterogeneous wireless networking between vehicles and roadside units in the cities of Clemson and Greenville, which we have used to evaluate different connected vehicle applications, such as traffic data collection, collision warning and queue warning for other funded research projects. In this task, we will develop several real world cyber-attack scenarios to test the effectiveness of security counter-measures developed in previous tasks. Depending on the real world performance, the solutions will be further refined to improve their performance.

Task 5: Preparation of Final Report

The research team will develop quarterly progress reports for submission to the Southeastern Transportation Center (STC), and all research findings will be incorporated in a final draft report for STC review comments. The revised final report will be submitted to the STC by addressing the comments.

5. Research Duration and Cost

The duration of this research project is 12 months. A timeline, with a proposed start date of May 02 2016 is presented in "Schedule/Timeline, Peer Review and Project Description" section, and provides specifics for each research task. The research team can adjust the project start date, if necessary.

Cost of the Project

Senior personnel: 0.25 month summer salary is requested for the PI, Dr. Mashrur Chowdhury to supervise the Clemson research team and research activities. 0.50 month summer salary is requested for Co-PI, Dr. Hongxin Hu to conduct research activities. 1.16 months salary is requested for the Co-PI, Dr. Kakan Dey to conduct research activities.

Other personnel: One graduate research assistant (10 hours) is requested for one year.

Fringe benefits: Fringe benefits are negotiated with DHHS and are calculated as follows: faculty fringe is 30.1%, 12 months employees is 36.3% and 8.2% for students.
http://www.clemson.edu/cfo/comptroller/rates/index.html

Other direct costs: Tuition Remission is charged at $10,523 per student with an annual increase of 5% as per Clemson University's policy. $1,700 is request for travel to conferences presenting research findings. $181 is requested for materials and supplies
http://www.grad.clemson.edu/programs/tuition.php

Facilities and administrative costs: F&A costs are calculated in accordance with Clemson University's policy at a rate of 26% as per Sponsor policy.
http://www.clemson.edu/cfo/comptroller/rates/index.html

Cost sharing

Senior personnel: Clemson is releasing the PI, Dr. Chowdhury's 2.2% time and the Co-PI, Dr. Hu's 5.6% time, Co-PI, Dr. Dey's 8.3% time to work on this project.

Other personnel: The graduate student's salary will be matched in the amount of $10,000 plus fringe.

Fringe benefits: Fringe benefits are negotiated with DHHS and are calculated as follows: faculty fringe is 30.1%, 12 months employees is 36.3% and 8.2% for students.
http://www.clemson.edu/cfo/comptroller/rates/index.html

Other direct costs:

Facilities and administrative costs: F&A costs are calculated in accordance with Clemson University's policy at a rate of 50% MTDC, PRED, 11, DHHS. Clemson is using the unrecovered indirect ($8,146) and the indirect on the cost share ($14,267) as cost share.
http://www.clemson.edu/cfo/comptroller/rates/index.html

6. Qualification of a research team

Dr. Ronnie Chowdhury, P.E., F.ASCE, (PI) from Clemson University, currently serves as the Eugene Douglas Mays Endowed Professor of Transportation in the Glenn Department of Civil Engineering at Clemson University. He is also a professor in the Department of Automotive Engineering at Clemson University and a member of the Clemson University International Center of Automotive Research (CU ICAR). Dr. Chowdhury leads the Roadway, Driver and Traffic Group in the Clemson University's Connected Vehicle Technology (CVT) Consortium. Dr. Chowdhury is also the Co-Director of the Complex Systems, Data Analytics and Visualization

Institute (CSAVI) at Clemson University, which focuses on research and education of Big Data Analytics for transportation and automotive systems.

Dr. Chowdhury has established himself as an educator and operational expert in transportation security and traffic operations, and served as a consultant for several public transportation agencies as a senior systems engineer for Iteris, Inc. and as a senior engineer for Bellomo-McGee, Inc. (BMI). Dr. Chowdhury is the co-author of two textbooks on ITS systems, the first with Dr. Adel Sadek entitled "Fundamentals of Intelligent Transportation Systems (ITS) Planning," which was published by Artech House in April 2003; and second with Drs. Ryan Fries and Jeffrey Brummond, entitled "Transportation Infrastructure Security Utilizing Intelligent Transportation Systems" which was published by Wiley and Sons in 2008.

Dr. Chowdhury has published his research results in Transportation Research Records, the American Society of Civil Engineers (ASCE) Journal on Infrastructure Systems, the ASCE Journal on Transportation Engineering, Reliability Engineering and System Safety, and the Journal for the Institute of Transportation Engineers (ITE). He is the past chair of the American Society of Civil Engineers Committee on Computing in Transportation, a member of the Transportation Research Board Committees on Artificial Intelligence and Visualization in Transportation, and ASCE Committees on Transportation Safety and Advanced Transportation Technology.

Dr. Hongxin Hu (Co-PI) is an assistant professor in the School of Computing at Clemson University. Dr. Hu received his Ph.D. degree in computer science and engineering from Arizona State University in 2012. Dr. Hu's research interests centrally focus on the area of cybersecurity. More specifically, Dr. Hu strives to develop effective solutions to address realistic security issues created by today's emerging technologies and systems, such as software-defined networking, social networks, mobile computing, cloud computing, and healthcare systems. Dr. Hu has published over 70 refereed technical papers, many of which appeared in top conferences, and top journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics & Security, IEEE Transactions on Knowledge and Data Engineering. Dr. Hu's paper "RiskMon: Continuous and Automated Risk Assessment of Mobile Applications" was published in proceedings of the 4th ACM Conference on Data and Application Security and Privacy (CODASPY) in 2014. The paper won the **Best Paper Award**. In 2013, Dr. Hu's paper named "On the Security of Picture Gesture Authentication" was published in proceedings of the 22nd USENIX Security Symposium (USENIX Security). USENIX Security is a top security conference focusing on computer system security. The research presented in this paper has attracted massive **media coverage** including *ACM TechNews*, *InformationWeek*, *NetworkWorld*, *Slashdot*, and *PCWorld* in August & September 2013.

Dr. Hu recently also worked on *security in advanced communication networks*. Specifically, Dr. Hu introduced a new firewall system for emerging Software-Defined Networking (SDN). In recognition of the important contributions of FlowGuard, Dr. Hu's paper entitled "FlowGuard: Building Robust Firewalls for Software-Defined Networks" was recently published in proceedings of the ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN) in 2014. Dr. Hu's paper entitled "Detecting and Resolving Firewall Policy Anomalies" has been published in IEEE Transactions on Dependable and Secure Computing (TDSC) in 2013.

TDSC is a top journal in the field of computer security and privacy. The paper has been cited 76 times by different publications in the world after two years.

Dr. Kakan Dey (Co-PI) is a post-doctoral fellow on connected and automated vehicle technology in the Glenn Department of Civil Engineering at the Clemson University. He also received his Ph.D. degree in May, 2014 from Clemson University and his M.S. degree in May, 2010 from Wayne State University. The SCDOT project related to his Ph.D. research was selected by AASHTO as a "High Value Research Project" in 2014. Currently, Dr. Dey is engaged in research on a project with peers in the Clemson School of Computing to evaluate the reliability of heterogeneous wireless communication for traffic data collection. He also led a team of researchers at Clemson in the development of connected vehicle applications using DSRC and LTE communication technologies, which were demonstrated in the ITS Carolinas Annual Meeting 2015 in Charlotte, North Carolina.

Dr. Dey conducted research to identify the crash causal factors for emergency vehicle crashes and developed recommendations to improve emergency vehicle safety in Michigan. He also worked on several research projects in Michigan to improve pedestrian safety through education and enforcement, identification of countermeasures for intersection and corridor safety deficiencies through crash analysis, and evaluation of the effectiveness of an emergency vehicle safety alert system. While at Clemson he has participated in two SCDOT sponsored safety studies, one of which involved the use of fault-tree analysis to estimate tort liability risks of SCDOT, and the other on assessing safety impacts of roadway access management policies. Dr. Dey's project on tort liability was also selected by the AASHTO as a "High Value Research Project" in 2012.

Principal Investigator, Dr. Chowdhury will oversee the research activities, and provide technical guidance to other two Co-PIs and students. The team will meet weekly to review weekly progress and develop immediate goals. Furthermore, as requested by Southeast Transportation Center (STC), Dr. Chowdhury and Dr. Hu will

1. Develop and submit an implementation plan for the planned outcomes, upon award of an O/E Grant;
2. Submit at least two papers based on the research project to a peer-reviewed journal;
3. Issue a press release announcing the final results of the research;
4. Present research results to an academic or professional group and submit the presentation to the STC for posting on the website;
5. Provide quarterly reports to STC on the research.

7. STUDENT INVOLVEMENT

One graduate student will work on this project for 20 hours per week for a year. This research project will be a part of his/her M.S. thesis. Interested undergraduate students will be recruited under creative inquiry program to acquire cutting edge research experiences.

8. TECHNOLOGY TRANSFER

The research team will develop and maintain a google site that will include detailed information about the project with outcomes from each task of the project. This public website will also include comments page on which professionals can log in and provide their inputs based on the published outcomes.

9. Schedule/Timeline, Peer Review and Project Description

Table 1: Schedule Timeline

Task/Month	1	2	3	4	5	6	7	8	9	10	11	12
Task 1: V2I Security Threat Review and Measurement												
Task 2: CVGuard Platform Development for Attack Capturing, Analysis and Countermeasure Implementation												
Task 3: Evaluation of the CVGuard through Simulation Experiments												
Task 4: Field Evaluation												
Task 5: Preparation of Final Report												

*Milestones- end of each task, working report will be submitted

STC Research Project Description

Project Title: Development of a Security Platform for Vehicle to Infrastructure Network

Principal Investigator: Mashrur (Ronnie) Chowdhury
University: Clemson University
Telephone: 864-656- 3313 **Email Address:** mac@clemson.eu

External Project Contact (if applicable):
Address Street:
City: **State:** **Zip:**
Telephone: **Email Address:**

Project Start Date: May 02, 2016 **End Date:** May 01, 2017
Other Milestones, Dates:
Task 1: V2I Security Threat Review and Measurement- August 01, 2016, **Task 2:** CVGuard Platform Development for Attack Capturing, Analysis and Countermeasure Implementation- October 01, 2016, **Task 3:** Evaluation of the CVGuard through Simulation Experiments - January 01, 2017 , **Task 4:** Field Evaluation- March 01, 2017, **Task 5:** Preparation of Final Report- May 01, 2017
Project #:

Project Objective:
The objectives of this research are as follows:

- Develop CVGuard, a V2I security platform for discovering analyzing and implementing countermeasures for cyber-attacks;
- Perform field tests to evaluate the performance of the security solutions enabled by our security platform in the V2I interfaces.

Project Abstract:
Ensuring that the connected transportation ecosystem is cognizant of potential cyber-attacks is of the utmost importance. Specifically, ensuring the secure communication between diverse stakeholders in connected transportation systems is perhaps the major challenge to the safe and reliable system operations. The primary security risks may originate in different interface levels in connected transportation systems such as Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) or Infrastructure to Infrastructure (I2I). However, today's Information Technology (IT) security ecosystem, which relies on a combination of static perimeter network defenses (e.g., firewalls and intrusion detection/prevention systems), ubiquitous use of end-host based defenses (e.g., antivirus), and software patches from vendors (e.g., Patch Tuesday), is fundamentally ill-equipped to handle the security issues in the connected vehicle ecosystem. In this research, we propose to build a flexible and reliable security protection mechanism, called CVGuard, leveraging emerging network techniques that support the development of V2I security solutions. We will develop diverse security threat scenarios in a V2I communication environment and evaluate the performance of CVGuard through simulations and field tests. Outcomes of our research will provide a much-needed guidance to establish a secure and resilient communication infrastructure for future connected vehicle technology deployments in the real world.

Task Description:

Task 1: V2I Security Threat Review and Measurement, **Task 2:** CVGuard Platform Development fo Capturing, Analysis and Countermeasure Implementation, **Task 3:** Evaluation of the CVGuard through Simulation Experiments, **Task 4:** Field Evaluation, **Task 5:** Preparation of Final Report

Total Budget: $ 49,850 (with equal cost sharing from Clemson University fund)

Student Involvement (Thesis, Assistantships, Paid Employment):
One graduate student will work on this project for 20 hours per week for a year. This research project will be a part of his/her M.S. thesis. Interested undergraduate students will be recruited under the CU Creative Inquiry program to acquire cutting edge research experiences.

Relationship to Other Projects:
Currently, we are deploying the first connected vehicle testbed for heterogeneous wireless communication for CV applications, funded by the National Science Foundation. We plan to use the testbed resources in Task 4 in addition to our existing CV infrastructure, which includes a heterogeneous wireless network and connected in-vehicle and roadside equipment in Clemson, South Carolina.

Technology Transfer Activities:
The research team will develop and maintain a google site that will include detailed information about the project with outcomes from each project task. This public website will also include comments page through which professionals may log in and provide their inputs based on the published outcomes. We will also publish our results in major journals and present out finding in conferences.

Potential Benefits of Project:
Secure V2V, V2I and I2I communication network is necessary for ensuring user acceptance of this technology, and enable the numerous safety benefits of this technology. In this research, we will develop the security solution known as CVGuard to enable secure V2I communication, which will ensure the safe operation of CV applications and will enable diverse CV safety, mobility and environmental applications.

TRB Keywords:
Connected vehicle, security, safety, communication

PEER REVIEW FORM

Peer Reviewer #1

Name:	Adel W. Sadek
Organization/University Affiliation:	University at Buffalo
Address:	220 Ketter Hall, Buffalo, NY 14260
Phone #:	(716) 645-4367
Fax #:	(716) 645-3733
Email address:	asadek@buffalo.edu
Please submit a brief overview of why this individual is qualified to review the material.	
Qualifications of reviewer: Adel W. Sadek is a Professor of Civil, Structural and Environmental Engineering at the University at Buffalo (UB). He also serves as the Director of UB's Institute for Sustainable Transportation and Logistics, Director of the Transportation Informatics Tier I University Transportation Center, and Chair of UB2020's Strategic Strength in Extreme Events. Dr. Sadek is the recipient of a National Science Foundation (NSF) CAREER award, and a 2011 IBM Smarter Planet Faculty Innovation Award. His primary research expertise includes data analytics in intelligent transportation systems, safety and security of connected transportation systems.	

Peer Reviewer #2

Name:	Yuanchang Xie
Organization/University Affiliation:	University of Massachusetts Lowell
Address:	One University Avenue, Lowell, MA 01854
Phone #:	(978) 934-3681
Fax #:	(978) 934-3052
Email address:	yuanchang_xie@uml.edu
Please submit a brief overview of why this individual is qualified to review the material.	
Qualifications of reviewer: Dr. Xie is an Assistant Professor with the Department of Civil and Environmental Engineering, University of Massachusetts (UMass) Lowell, Lowell, MA, USA. Prior to joining UMass Lowell in 2011, he was with South Carolina State University, Orangeburg, SC, USA, as an Assistant Professor for 3.5 years. His research focuses on traffic flow modeling, traffic control and simulation, intelligent transportation systems, traffic safety, GIS-T, connected vehicle technology, big data in transportation, and applications of artificial intelligence and operations research in transportation. Dr. Xie is a member of the Transportation Research Board's (TRB) Transportation Safety Management Committee (ANB10) and Transportation of Hazardous Materials Committee (AT040). He is also actively involved in the TRB Artificial Intelligence and Advanced Computing Applications (ABJ70) Committee.	

Peer Reviewer #3

Name:	Ping Yi
Organization/University Affiliation:	University of Akron
Address:	ASEC 213, Akron, OH 44325
Phone #:	330-972-7294
Fax #:	330-972-6020
Email address:	pyi@uakron.edu
Please submit a brief overview of why this individual is qualified to review the material.	
Qualifications of reviewer: Dr. Yi is a Professor with Civil Engineering at the University of Akron, Ohio, USA. Dr. Yi has been working in the transportation engineering field for nearly 20 years. His areas of research include traffic operations and control, traffic safety, and application of advanced technologies in the intelligent transportation systems. His research interest incudes Advanced Traffic Sensor Evaluation and Analysis, Data Mining and Data Fusion, Traffic Responsive and Adaptive Signal Control Systems, Location-Based Information Systems, Traffic Safety.	

10. Budget

Southeastern Transportation Center
Proposed Budget
O/E Grant 2014-2015

Title: Development of a Security Platform for Vehicle to Infrastructure Network

University: **Clemson University**

	Federal Funds	Matching Funds
Salaries:		
Faculty	9,176	8,417
Administrative Staff		
Other Staff	4,822	4,157
Graduate Student Salaries/Stipends	10,000	10,000
Undergraduate Student Salaries/Stipends		
Total Salaries/Stipends		
Benefits (including student health insurance)	5,333	4,863
Total Salaries and Benefits	**29,331**	**27,437**
Other Direct Costs:		
Permanent Equipment		
Expendable Equipment and Supplies	181	
Computer Costs		
Non-salary Education Costs – tuition/fees		
Other Costs: (specify)		
Printing / duplication		
Postal expense		
Communication		
Conference Registration / Fees		
Travel	1,700	
Computer Costs		
Other miscellaneous costs: Tuition	10,523	
Total Other Direct Costs	**12,404**	
	41,735	27,437
Indirect Costs at 26% /24% on C/S	**8,115**	**8,146**
Unrecovered at 50%		14,267
TOTAL COSTS	**49,850**	**49,850**

Appendices

REFERENCES

[1] NHTSA, Fatality analysis reporting system (FARS) encyclopedia, http://www-fars.nhtsa.dot.gov/Main/index.aspx. Accessed on February 10, 2016.

[2] S. Singh, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey," Report No # DOT HS 812 115, 2015.

[3] USDOT, "Connected Vehicle Research," 2015. http://www.its.dot.gov/connected_vehicle/connected_vehicles_FAQs.htm. Accessed on February 10, 2016.

[4] National Vulnerability Database, https://nvd.nist.gov/. Accessed on February 10, 2016.

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[6] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: network intrusion detection and countermeasure selection in virtual network systems," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 198–211, 2013.

[7] Ns-3, Network Simulator- 3, https://www.nsnam.org/. Accessed on February 10, 2016.

Resumes

Mashrur (Ronnie) Chowdhury, Ph.D., P.E., F. ASCE, IEEE Senior Member

Eugene Douglas Mays Professor of Transportation
Professor of Civil Engineering, Professor of Automotive Engineering
216 Lowry Hall, Clemson University, Clemson, SC 29634
Phone: (864) 656-3313; Fax: (864) 656-2670, Email: mac@clemson.edu

Professional Preparation

University of Virginia, Charlottesville, VA	Civil Engineering	Ph.D. 1995
Morgan State University, Baltimore, MD	Transportation	M.S. 1991
Bangladesh Institute of Technology, Bangladesh	Civil Engineering	B.S. 1988

Appointments

Clemson University

August 2012 – Present	Professor of Civil Engineering, Professor of Automotive Engineering
January 2011 – Present	Eugene Douglas Mays Professor of Transportation Engineering
August 2010 – December 2010	Ideas Professor, College of Engineering and Science
August 2008 – August 2012	Associate Professor, Civil Engineering
August 2004 – August 2008	Assistant Professor, Civil Engineering

University of Dayton

August 2000 – May 2004	Assistant Professor, Civil Engineering

Iteris, Inc., Sterling, VA

March 1997 – August 2000	Senior Systems Engineer

Bellow-McGee Inc. (BMI), Vienna, VA

January 1996 – March 1997	Senior Engineer
June 1994 – December 1995	Engineer II

University of Virginia, Center for Risk Management of Engineering Systems

December 1991 – May 1994	Research Assistant
1991	Graduate Research Fellow, FHWA
1990	Engineering Intern, Maryland State Highway Administration

Textbooks

[1] Fries, R., Chowdhury, M., and Brummond, J., "*Transportation Infrastructure Security Utilizing Intelligent Transportation Systems,"* John Wiley & Sons, ISBN-10**:** 0470286296 (2008).

[2] Chowdhury, M., and Sadek, A., "*Fundamentals of Intelligent Transportation Systems Planning*," Artech House, Inc., Norwood, MA, ISBN # 1-58053-160-1, (2003).

Most Relevant Publications to the Proposed Project

[1] Lantz, K., Khan, S., Ngo, L. B., Chowdhury, M., Donaher, S., and Apon, A., "Potentials of Online Media and Location-based Big Data for Urban Transit Networks in Developing Countries," *Transportation Research Record: Journal of the Transportation Research Board,* (2015). In-press.

[2] Dey, K., Mishra, A., and Chowdhury, M., "Potential of Intelligent Transportation Systems in Mitigating Adverse Weather Impacts to Road Mobility: A Review," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, No. 3, pp 1107 - 1119, (2015).

[3] Tupper, L., Bausman, D., Chowdhury, M., and Bhavsar, P., "Development of a Professional Services Management Training Program," *Transportation Research Record: Journal of the Transportation Research Board*, Vol. 2414(1), pp 29-34, (2014).

[4] Johnson, J., Chowdhury, M., He, Y., and Taiber, J., "Utilizing Real-Time Information Transferring Potentials to Vehicles to Improve the Fast-Charging Process in Electric Vehicles," *Transportation Research Part C: Emerging Technologies,* Vol. 26, pp 352–366, (2013).

[5] Fries, R., Anjuman, T. and Chowdhury, M., "Selecting an Asset Management System for Intelligent Transportation Systems," *Public Works Management & Policy,* Vol. 18, Issue 4, pp 322-337, (2013).

[6] Fries, R., Gahrooei, M., Chowdhury, M., and Conway, A., "Meeting Privacy Challenges While Advancing Intelligent Transportation Systems," *Transportation Research Part C: Emerging Technologies,* Vol. 25, pp 34–45, (2012).

[7] Fries, R., Hamlin, C., Chowdhury, M., Ma, Y., and Ozbay, K., "Operational Impacts of Incident Quick Clearance Legislation: A Simulation Analysis," *Journal of Advanced Transportation*, Vol. 46, Issue 1, pp 1-11, (2012).

[8] Zhou, Y., Chowdhury, M., Wang, K.C., Bhide, V. and Fries, R., "On-Line Traffic Surveillance: Impacts of Wireless Communications on Video Quality," ASCE *Journal of Transportation Engineering,* Vol. 138, No. 5, (2012).

[9] Ma, Y., Fries, R., Chowdhury, M., and Inamdar, I., "Evaluation of Integrated Allocation of Intelligent Transportation Systems (ITS) Technologies Using Stochastic Incident Generation and Resolution Modeling," *Simulation: Transactions of the Society for Modeling and Simulation International*, Vol. 88, No. 1, pp 123-133, (2012).

[10] Fries, R., Chowdhury, M., Ma, Y., and Stephens, L., "Evaluation of Different Contraflow Strategies for Hurricane Evacuation in Charleston," *Journal of Planning and Technology,* Vol.34, Issue 2, pp 139-154, (2011).

[11] Ma, Y., Chowdhury, M., Jeihani, M., and Fries, R., "Accelerated Incident Detection across Transportation Networks using Vehicle Kinetics and Support Vector Machine (SVM) in Cooperation with Infrastructure Agents," *IET ITS Journal,* Vol. 4, Issue 4, pp 328 -337, (2010).

[12] Fries, R., Chowdhury, M., and Dunning, A., "Incident Detection with Traffic Sensors on Urban Highways," *ITE Journal*, Vol. 79, No. 8, pp 69-74, (2009).

[13] Ma, Y., Zhou, Y., Chowdhury, M., Wang, K.C., and Fries, R., "A Framework for Performance Evaluation of Communication Alternatives for Intelligent Transportation Systems," *Journal of Intelligent Transportation Systems,* No. 13 (3), pp 111-126, (2009).

[14] Fries, R., Chowdhury, M., and Trummel, H., "Liabilities of Public Agencies for Intelligent Transportation Systems Projects," *ITE Journal,* Vol. 78, No. 7, pp 69-73, (2008).

[15] Fries, R., Chowdhury, M., Dunning, A., and Boyles, B., "Transportation Security Framework for a Medium-Size City," *European Journal of Transport and Infrastructure Research (EJTIR),* Vol. 8, Issue 1, pp 1-16, (2008).

[16] Fries, R., Inamdar, I., Chowdhury, M., Taaffe, K., and Ozbay, K., "Feasibility of Traffic Simulation for Decision Support in Real-time Regional Traffic Management," *Transportation Research Record: Journal of the Transportation Research Board*, No. 2035, pp 169-176, (2007).

[17] Bhavsar, P., Chowdhury, M., Sadek, A., Sarasua, W., and Ogle, J., "Decision Support System for Predicting Traffic Diversion Impact across Transportation Networks using Support Vector Regression," *Transportation Research Record: Journal of the Transportation Research Board*, No. 2024, pp 100-106, (2007).

[18] Chowdhury, M., Sadek, A., Ma, Y., Kanhere, N., and Bhavsar, P., "Applications of Artificial Intelligence Paradigms to Decision Support in Real-time Traffic Management," *Transportation Research Record: Journal of the Transportation Research Board*, No. 1968, pp 92-98, (2006).

Synergistic Activities

- Associate Editor, IEEE Transactions on Intelligent Transportation Systems, IEEE
- Associate Editor, Journal of Intelligent Transportation Systems, Taylor and Francis
- Editorial Advisory Board Member, Transportation Research Part C, Elsevier
- Coauthor of 2 intelligent transportation systems related textbooks (first in 2003 and second in 2008)
- Summer Research Mentor, South Carolina Governor's School for Science and Mathematics students, 2006, 2007, 2009, and 2012

Honors and Awards

Wilbur Smith Distinguished Transportation Educator Award, 2015; AASHTO High Value Research Project, 2014, 2012; Faculty Mentoring Award, College of Engineering and Science, Clemson University, 2013; McQueen Quattlebaum Faculty Achievement Award, College of Engineering and Science, Clemson University, May, 2012; IDEAS Professor, College of Engineering and Science, Clemson University, May, 2010.

Hongxin Hu, Ph.D.
Assistant Professor
Division of Computer Science, School of Computing Clemson University
Clemson, SC 29634
Email address: hongxih@clemson.edu
WWW home page: http://www.cs.clemson.edu/~hongxih
Office phone: (864) 656 2847

PROFESSIONAL PREPARATION

China University of Geosciences, Wuhan, China, Computer Science, B.S. 1997

China University of Geosciences, Wuhan, China, Computer Science, M.S. 2002

Arizona State University, Tempe, AZ, Computer Science and Engineering, Ph.D. 2012

ACADEMIC/PROFESSIONAL APPOINTMENTS

- Assistant Professor, School of Computing, Clemson University, July 2014 – Present
- Assistant Professor, Department of Computer and Information Sciences, Delaware State University, August 2012 – June 2014
- Lecturer, College of Computer Science, China University of Geosciences, China, July 2002 – December 2004
- Assistant, College of Computer Science, China University of Geosciences, China, August 1997 – July 2002

SELECTED PRODUCTS (* indicating student authors) Most Relevant

1. Juan Deng*, **Hongxin Hu**, Hongda Li*, Zhizhong Pan*, Kuang-Ching Wang, Gail-Joon Ahn, Jun Bi and Younghee Park, "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls", *Proc. of IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN*), San Francisco, USA, November 18-21, 2015.

2. Shuyong Zhu*, Jun Bi, Chen Sun*, Chenghui Wu* and **Hongxin Hu**, "SDPA: Enhancing Stateful Forwarding for Software-Defined Networking", *Proc. of the 23rd IEEE International Conference on Network Protocols (ICNP)*, San Francisco, USA, November 10-13, 2015. (**Best Paper Nominee**)

3. Jun Bi, Shuyong Zhu*, Guang Yao*, Chen Sun*, **Hongxin Hu**, "Supporting Virtualized Network Functions with Stateful Data Plane Abstraction", *IEEE Network* (to appear).

4. **Hongxin Hu**, Wonkyu Han*, Gail-J. Ahn and Ziming Zhao*, "FlowGuard: Building Robust Firewalls for Software-Defined Networks," *Proc. of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN)*, Chicago, IL, USA, August 22, 2014.

5. **Hongxin Hu**, Gail-J. Ahn and Ketan Kulkarni*, "Detecting and Resolving Firewall Policy Anomalies," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Vol. 9, No. 3, 2012.

Other Related

1. **Hongxin Hu**, Wonkyu Han, Gail-J. Ahn and Ziming Zhao, "Towards a Reliable SDN Firewall," *Proc. of Open Networking Summit 2014 (ONS) Research Track*, Santa Clara, California, USA, March 3-5, 2014.
2. Wonkyu Han, **Hongxin Hu** and Gail-J. Ahn, "LPM: Layered Policy Management for Software- Defined Networks*," Proc. of the 28th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec),* Vienna, Austria. July 14-16, 2014.
3. **Hongxin Hu**, Gail-J. Ahn and Ketan Kulkarni, "FAME: A Firewall Anomaly Management Environment," *Proc. of ACM CCS Workshop on Assurable & Usable Security Configuration (SafeConfig*), Chicago, IL, USA, October 4, 2010.
4. **Hongxin Hu**, Gail-J. Ahn and Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," *IEEE Transactions on Knowledge and Data Engineering (TKDE),* Vol. 25, No. 7, July, 2013. (**Featured by the IEEE Special Technical Community on Social Networking**)
5. Ziming Zhao, Gail-J. Ahn, Jeong-Jin Seo and **Hongxin Hu**, "On the Security of Picture Gesture Authentication", *Proc. of 22nd USENIX Security Symposium (USENIX Security)*, Washington DC, August 2013. (**Media Coverage: ACM TechNews, InformationWeek, etc**)
6. Yan Zhu, Gail-Joon Ahn, **Hongxin Hu**, Changjun Hu and Di Ma, "Role-Based Cryptosystem: A New Cryptographic RBAC System Based on Role-Key Hierarchy", IEEE Transactions on Information Forensics & Security (TIFS), Vol. 8, No. 12, December, 2013.
7. H**ongxin Hu**, Gail-Joon Ahn and Ketan Kulkarni, "Discovery and Resolution of Anomalies in Web Access Control Policies", IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 10, No. 6, November/December, 2013. (Selected as the spotlight paper of the issue)
8. Juan Wang, **Hongxin Hu**, Bo Zhao, Fei Yan, Huangguo Zhang and Qianhong Wu, "Formal Analysis of Information Card Federated Identity-Management Protocol", Chinese Journal of Electronics (CJE), Vol. 22, No. 1, January, 2013.
9. Yan Zhu, Mengyang Yu, **Hongxin Hu**, Gail-Joon Ahn and Hongjia Zhao, "Efficient Constructions of Provably Secure Steganography under Ordinary Covert Channels", SCIENCE CHINA - Information Sciences, Springer, Vol. 55, No. 7, July, 2012.

SYNERGISTIC ACTIVITIES

- Guided a team "FLOWGUARD" to win the third place in the **first annual Extreme SDN Innovation Challenge** in June 2015.
- Assigned to teach a Clemson University summer scholars class, Computer Security and Forensics. This program offers a summer enrichment program for gifted middle and high school students.
- Co-organized the U.S. Cyber Challenge Delaware Summer Cyber Security Camp. 47 students (including 3 high school students) attended this summer camp. It has attracted massive media coverage in July 2013. Guided a team "My Little Pwnies" (60% of female students) to win the Delaware U.S. Cyber Challenge Competition in July 2013.

- Served in several conference and workshop organizing roles, such as SACMAT 2013 & 2014 & 2015, CoolSDN 2014&2015, ICCCN 2015, GLOBECOM 2015 program committees, TrustCol 2014&2015 program co-chair, SACMAT 2014&2016 proceedings chair, and CCS 2014 web chair.
- Reviewer for ACM Transactions on Information and System Security, ACM Transactions on Software Engineering and Methodology, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Network and Service Management, IEEE Internet Computing, and Journal of Computer Security.

KAKAN C DEY, Ph.D.

Postdoctoral Fellow on Connected and Autonomous Vehicle Technology
Glenn Department of Civil Engineering, Clemson University, SC
351 Fluor Daniel Hall
(313) 523-0865, kdey@clemson.edu

Professional Preparation

Bangladesh University of Eng. & Tech, Bangladesh	Civil Engineering B.S. 2005
Wayne State University, Detroit, MI	Civil Engineering M.S. 2010
Clemson University, Clemson, SC	Civil Engineering Ph.D. 2014

Appointments

Postdoctoral Fellow, Clemson University, May 2014 – Present

Research Assistant, Clemson University, August 2010 to May 2014

Research Assistant, Wayne State University, January 2008 to December 2009

Engineer, Titas Gas T&D Co., Bangladesh, October 2006 to December 2007

Lecturer, Stamford University, Bangladesh, April 2006 to October 2006

Peer Reviewed Journal Publications

[1] Li, Z., **Dey, K.,** Chowdhury, M., and Bhavsar, P., (2015) "Connected Vehicle Technology Application for Dynamic Routing of Electric Vehicles in an Inductively Coupled Power Transfer Environment," *IET Intelligent Transport Systems Journal* (Accepted)

[2] Dunning, A., **Dey, K.,** and Chowdhury, M., (2015) "Review of Transportation Infrastructure Deterioration and Recovery Policies due to Overweight Truck and a Case Study on Stakeholders' Perspectives," ASCE *Journal of Infrastructure Systems* (In press)

[3] **Dey, K.,** Yan, L., Wang, X., Wang, Y., Shen, H., Chowdhury, M., Yu, L., Qiu, C., and Soundararaj, V., (2015) "A Review of Communication, Driver Characteristics and Controls Aspects of Cooperative Adaptive Cruise Control (CACC)," IEEE *Transactions on Intelligent Transportation Systems*, Published online, DOI: 10.1109/TITS.2015.2483063

[4] **Dey, K.,** Mishra, A., and Chowdhury, M., (2015) "Potential of Intelligent Transportation Systems in Mitigating Adverse Weather Impacts on Road Mobility: A Review," *IEEE transactions in ITS*, Vol. 16 (3), pp. 1107-1119, DOI: 10.1109/TITS.2014.2371455

[5] **Dey, K.,** Chowdhury, M., Wiecek, M., and Dunning, A., (2014) "Tradeoff Analysis for Offsetting Overweight Truck Damage Costs to transportation Infrastructure," *ASCE Journal of Transportation Engineering,* Vol. 141(7), 04015008

[6] **Dey, K.,** Chowdhury, M., Pang, W., Putman, B., and Chen, L., (2014) "Estimation of Pavement and Bridge Damage Costs Due to Overweight Trucks," *Transportation Research Record* , Vol. 2411, pp. 62-71

[7] Davis-McDaniel, C., Chowdhury, M., and Pang, W., and **Dey, K.,** (2013) "Fault-tree model for identification of causal factors and risk assessment of bridge failure," *ASCE Journal of Infrastructure Systems,* Vol. 19(3), pp. 326–334

Peer Reviewed Conference

[1] Rahman, M., Du, Y., Ngo, L., **Dey, K.,** Chowdhury, M., and Apon, A., (2016) "An Innovative way to Manage Data for Connected Vehicle Applications," In *95th Transportation Research Board Annual Meeting compendium of papers, Washington D.C.* (Accepted).

[2] Gende, M., Chowdhury, M., **Dey, K.,** and Sarasua, W., (2016) "Connected Vehicle Technology for Allowing Priority Requests at Signalized Intersections- An Analysis," In *95th Transportation Research Board Annual Meeting compendium of papers, Washington D.C.* (Accepted).

[3] **Dey, K.,** Putman, B., Chowdhury, M., and Bhavsar, P., (2015) "Quantification of Accelerated Pavement Serviceability Reduction Due to Overweight Truck Traffic" In *94th Transportation Research Board Annual Meeting compendium of papers*, Washington D.C.

[4] Rahman, M., Khan, S., Chowdhury, M., Huynh, N., Ogle, J., **Dey, K.,** and Bhavsar, P., (2015) Incident Command System Strategies for Incident Management on Freeways: Simulation Analysis," In *94th Transportation Research Board Annual Meeting compendium of papers, Washington D.C.*.

[5] Li, Z., **Dey, K.,** Chowdhury, M., and Bhavsar, P. (2014) "A Connected Vehicle Supported Routing Strategy for Electric Vehicles," *ITS World Congress 2014*, Detroit, Michigan.

[6] **Dey, K.,** Chowdhury, M., Pang, W., Putman, B., and Chen., L., (2014) "Transportation Infrastructure Damage Costs Due to Overweight Trucks and Corresponding Cost Recovery," In *93rd Transportation Research Board Annual Meeting compendium of papers*, Washington D.C.

[7] **Dey, K.,** Chowdhury, M., and Wiecek, M., (2014) "A Tradeoff Analysis for Different damage Fee Offsetting Overweight Truck Damage Costs," In *93rd Transportation Research Board Annual Meeting compendium of papers*, Washington D.C.

[8] Zhou, Y., Chowdhury, M., Wang, K., and **Dey, K.,** (2013) "Evaluation of wireless communication performance between adjacent nodes for roadway traffic management applications," In *Transportation Research Board Annual Meeting compendium of papers*, Washington D.C.

[9] Davis-McDaniel, C., Chowdhury, M., Pang, W., and **Dey, K.,** (2012) "Identification of causal factors of bridge failure through fault-tree analysis," In *Transportation Research Board Annual Meeting compendium of papers*, Washington D.C.

Synergistic Activities

- Member, ASCE Intermodal & Logistics Committee
- Member, Transportation Research Board
- Reviewers, Transportation Research Board Annual Meeting & Transportation Research Record, IEEE transaction on Intelligent Transportation Systems, Journal of Intelligent Transportation Systems, Transportation Research Record Part C, ITS world congress.
- Co-Advisor, Clemson IEEE ITS Student Chapter