Securing Wireless Communications of Connected Vehicles with Artificial Intelligence

Prinkle Sharma, Hong Liu*, Honggang Wang, and Shelley Zhang†
Department of Electrical and Computer Engineering
†Department of Computer and Information Science
University of Massachusetts, Dartmouth, U.S.A.
{PSharma1, HLiu, HWang1, X2Zhang}@UMassD.edu
*Corresponding Author

***Abstract*—This work applies artificial intelligence (AI) to secure wireless communications of Connected Vehicles. Vehicular Ad-hoc Network (VANET) facilitates exchange of safety messages for collision avoidance, leading to self-driving cars. An AI system continuously learns to augment its ability in discerning and recognizing its surroundings. Such ability plays a vital role in evaluating the authenticity and integrity of safety messages for cars driven by computers. Falsification of meter readings, disablement of brake function, and other unauthorized controls by spoofed messages injected into VANET emerge as security threats. Countermeasures must be considered at design stage, as opposed to afterthought patches, effectively against cyber-attacks. However, current standards oversubscribe security measures by validating every message circulating among Connected Vehicles, making VANET subject to denial-of-service (DoS) Attacks. This interdisciplinary research shows promising results by searching the pivot point to balance between message authentication and DoS prevention, making security measures practical for the real-world deployment of Connected Vehicles. Message authentication adopts Context-Adaptive Signature Verification strategy, applying AI filters to reduce both communication and computation overhead. Combining OMNET++, a data network simulator, and SUMO, a road traffic simulator, with Veins, an open source framework for VANET simulation, the study evaluates AI filters comparatively under various attacking scenarios. The results lead to an effective design choice of securing wireless communications for Connected Vehicles.**

Keywords*—Resilience to denial-of-service (DoS) attacks, artificial intelligence (AI) for augmented cognitive capability, Connected Vehicles, Vehicular Ad-hoc Network (VANET), position and tracking, message authentication, signature verification, wireless communication

I. Introduction

The Internet of Things makes cars more connected in today's burgeoning technology of vehicular automation. The proliferation of sensors that collect huge amounts of data transforms cars into mobile platforms for endless applications and services. Connected Vehicles are becoming reality with ten million hitting the road in 2020, estimated by Business Insider Intelligence recently. Technology companies take a big piece from the pie, such as Google's public commitment to Self-Driving Car Project and Apple's mysterious strategy on iCar. Startups market for driverless cars, including Tesla on environmental-friendly electric motors. In addition, suppliers, like Delphi Automotive and Mobileye, develop turnkey systems for automakers to build into their vehicles. Massachusetts Department of Transportation, along with the Executive Office of Housing and Economic Development, made a bold announcement, at the Listening Session for "Testing, Deployment, and Development of Self-Driving Vehicles in Massachusetts" on 27 April 2016, to promote the state the Testbed of Driverless Vehicles for the nation.

Connected Vehicles impact the society by releasing human from driving. According to the National Highway Traffic Safety Administration, over thirty thousand people die in motor vehicle accidents in the United States alone every year <crashstats.nhtsa.dot.gov>. When cars driven by computers, however, security posts significant challenges. In 2015, a news shocked the nation that hackers remotely took control of a Jeep and killed its engine in motion on the highway [1]. The situation is not as dire as it sounds: the driver is a Wired magazine reporter working with security researchers Charlie Miller and Chris Valasek to show the vulnerability of modern vehicles. Sadly, in 2016, Tesla lost an employee while testing its self-driving car due to computer malfunction [2].

This work explores the effectiveness of artificial intelligence (AI) in securing communications among Connected Vehicles. An AI system learns from experience to augment its cognitive capability about its environment continuously and to make good decisions instantaneously [3]. Vehicular Ad-hoc Network (VANET) deployed by Connected Vehicles expands security vulnerability inherited from wireless communications, particularly in message spoofing and denial-of-service (DoS) attacks. This paper proposes AI predictive algorithms based on Bayes theory like Kalman and Particle Filter along with generic filters to detect spoofed messages with resilience to DoS attacks. Utilizing the features unique to surface transportation, the security scheme adopts context-adaptive signature verification strategy, significantly reducing the computational overhead in authenticating safety messages. Selective validation of beacon messages protects VANET against DoS attacks without losing the effectiveness of faulty message detection. The results ensure secure communications for vehicles to vehicles (V2V) and vehicles to infrastructures (V2I).

This research is sponsored in part by the University of Massachusetts President's Office for Cybersecurity Curriculum Initiation Funding and the Graduate Studies Office at the University of Massachusetts Dartmouth for Doctoral Support and Graduate Student Travel Grant.

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

II. Architecture of Connected Vehicles

Vehicles connect to each other wirerlessly with Vehicular Ad-hoc Network (VANET), a trending technology that takes moving cars as communication nodes to form a spontanous network. Routers, strategically placed along the road, ensure constant coverage for vehicular communications, possibly blanketing an entire city [4]. Fig. 1 illustrates the architecture of Connected Vehicles with VANET, where cars "talk" to each other and/or the networking infrustructure. On-Board Units (OBU) equipped on vehicles enable cars to communicate. Road-Side Units (RSU) expand communications with both spacial coverage and high data speed. A spetrum of Dedicated Short-Range Communication (DSRC) is assigned for VANET. Prior to market penetration, Connected Vehicles also work with cars of no OBUs being equipped via sensors, such as RAdio Detection And Ranging (RADAR) and LIght Detection And Ranging (LIDAR), to avoid collisions.

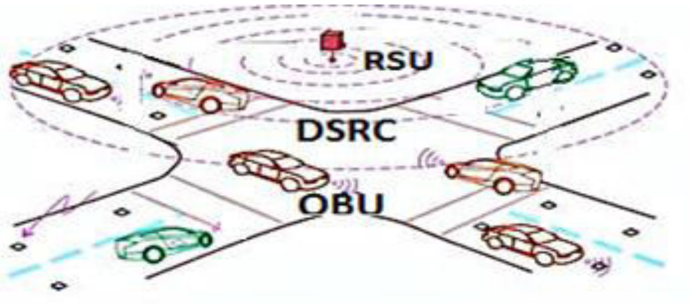

Fig. 1. Vehicular Ad-hoc Network (VANET)

An On-Board Unit (OBU) is based on WAVE standards including IEEE 802.11p, IEEE1609 (IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, IEEE 1609.11) and SAE J273. It is a special purpose computer with communication devices and sensors, augmenting control of Updated On-Board Diagnostics (OBD-II). OBD-IIs <www.obdii.com>, mendentory in autos since mid-90s, provide electronic means to control engine functions, monitor chassis and accessories including emission, and diagnose car problems. Fig. 2 shows a schematic diagram of a typical OBU excluding OBD-II. It consists of the control unit, the communication subsystem and the sensor network. Control and communication unit is based on the single board industrial PC of EPIC form (Embedded Platform for Industrial Computing).

The Central Control Unit acts as a heart of the whole system. The GPS unit and the sensors provides one-way communication which is necessary positioning, velocity and time, to enable location dependent co-operative services. The GSM unit is a two-way communication which ensures the mobile wireless communication among vehicle to vehicle and vehicle to infrastructure communication. The Central Control unit of OBU process and decrypt the information from upper layer and save it in flash memory to keep a track of all the neighboring vehicles behavior. Information Sharing broadcasts the vehicles location, speed and acceleration several times per second, which is got from GPS module.

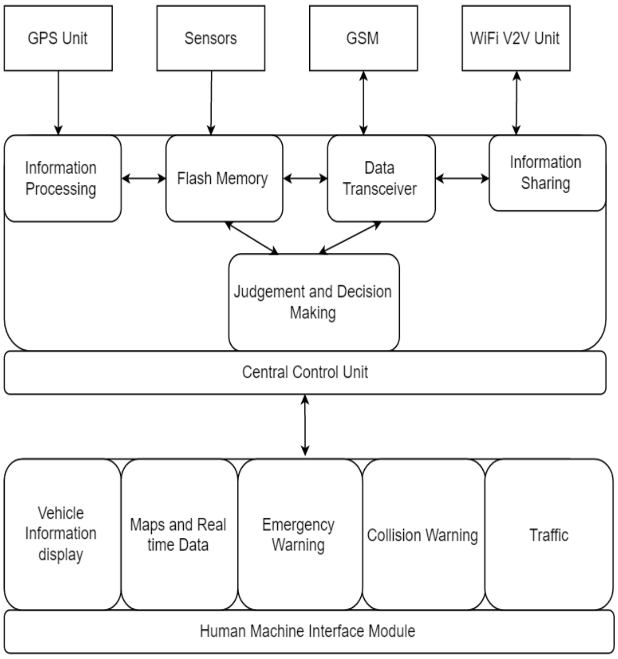

Fig. 2. On-Board Unit (OBU)

The Judgement and Decision Making block ensures to make a wise decision to ensure the security hence avoiding the attacks by false drivers. Human Machine Interface is the module which interact with the person sitting inside the car. LED's and a build in buzzer provides application feedback to the user and inform the status of the OBU. Information regarding vehicle speed, radio control, map view, emergency or collision warnings and traffic status is being shared with the user. User can get all the details displayed to his smartphone or a tablet via Bluetooth wireless link. If any hazard is encountered, then warning messages are being sent and controlled by application running on the user interface device.

A Road-Side Unit (RSU) functions like a stationary OBU powered by more computing resources and often with a wired connection to the Internet backbone. RSUs are usually installed at every 100-200 meters along a road to provide networking infrastructure for enhanced performance and enforced security in communications among Connected Vehicles.

Existing IEEE 802.11a compliant devices with data rates of up to 54 Mbps can support wireless communications among moving cars. However, varying speeds, dynamic traffics, and environmental constraints induce heavy overheads when traditional IEEE 802.11 MAC protocols operate in vehicular scenarios. To support V2V and V2I communications efficiently, the US Federal Communications Commission has assigned 75MHz of freely licensed spectrum in the 5.9GHz band for Dedicated Short Range Communication (DSRC) in VANET. The communication area covered by a DSRC module is limited to the maximum of 1Km diameter. The data transmission rates can be 9, 12, 18, 24, and 27 Mbps for 0 – 60km/h vehicle velocity and 3, 4.5, 6, 9, and 12 Mbps for 60 – 120 km/h vehicle velocity. The system uses BPSK, QPSK, 16-

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

QAM, or 64-QAM as the modulating mode [IEEE STD 802.11-2007].

The regional standards of DSRC by US is renamed to the international standards under IEEE 802.11p Wireless Access in Vehicular Environemnt (WAVE) as the ASTM 2313 working group for DSRC migrated to the IEEE 802.11 standard group. Fig. 3 depicts WAVE [5] in the Internet Protocol Stack. At the top Application Layer, IEEE 1609.1 defines protocols for both Safety Applications such as brake activations and Non-Safety Applications like traffic advices. The Transport Layer and Network Layer are tightly coupled because topological constraints by roads warrant simpler routing algorithms. They are lumped into IEEE 1609.3 with WAVE Management Entity (WME) as a management plane and WAVE Share Message Protocol (WSMP) as an operation plane compatible to traditional TCP/UDP for transport and IP for network. The Data Link Layer deals with the complexity of moving vehicle communications with divide and conquer: IEEE 1609.4 Upper Media Access Control Layer (UMAC) links between Logical Link Control Layer (LLC) and traditional IEEE 802.11 Lower Media Access Control Layer (LMAC). On the management plane, Data Link Layer contains management Entity (MXME) and Lower Media Acess Control Layer Management Entity (L-MLME). The Physical Layer uses IEEE 802.11a WAVE Physical Layer for operation and Physical Layer Management Entity (PLME) for management. The two protocols at the Physical Layer and the two lower media protocols at the Data Link Layer are collectively called IEEE 802.11p. Security is addressed across all the layers by IEEE 1609.2.

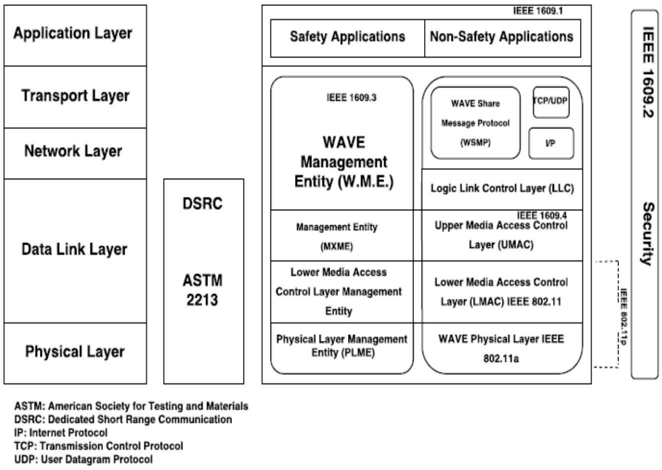
Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
DSRC
ASTM 2213
IEEE 1609.1
Safety Applications
Non-Safety Applications
IEEE 1609.3
WAVE Management Entity (W.M.E.)
WAVE Share Message Protocol (WSMP)
TCP/UDP
I/P
Logic Link Control Layer (LLC)
Management Entity (MXME)
IEEE 1609.4
Upper Media Access Control Layer (UMAC)
Lower Media Access Control Layer Management Entity
Lower Media Access Control Layer (LMAC) IEEE 802.11
Physical Layer Management Entity (PLME)
WAVE Physical Layer IEEE 802.11a
IEEE 802.11p
IEEE 1609.2
Security
ASTM: American Society for Testing and Materials
DSRC: Dedicated Short Range Communication
IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

Fig. 3. VANET in the Internet Protocol Stack

III. Security Challenges in Conncected Vehicles

The security of Connected Vehicles plays a pivotal role as their very existence relates to life threating situtions. It is important that the information or the program should not modified by the mallicious person. The privacy must be maintained such that the liablity of the driver is determined. The system should be reliable enough such that it doesn't share the important information with the false sources. For example, a malicious driver can send a false information of traffic jam or accident on a desired road to encourage other cars to avoid that route or by hacking the car system and make them work as the way they want. Also, in intelligent transportation systems, vehicles need only be with activity on the road. There are mainly two types of inter vehicle communications: naïve broadcasting and intelligent broadcasting [6].

In [7], Raya et al. describe a vehicular network model, an attacker model and a few attack types. They provide many solutions, e.g. digital signatures, tamper-proof device, key management, and anonymous public keys. Hsiao et. al. [8] try to solve the current VANET broadcast authentication standard that is vulnerable in signature flooding. Signature flooding is an event that excessive signature verification requests that exhause the computational resources of victims. Their paper propose two authentication schemes that can mitigate signature flooding attacks. However, till now the life threading security issue still persist and very little attention is paid on it. The following classical list of security requirements in computer networking can be applied to connected vehicles networks:

Confidentiality (Privacy)

Confidentiality or privacy ensures that only the sender and intended receiver comprehend transmitted message.

Message integrity

Message integrity requires the transmitted data between the sender and receiver is unchanged in transmission for whatever reasons. If we cannot guarantee that, we need to be able to detect modified messages.

End-point authentication

End-point authentication means that both sender and receiver are able to identify the other party involved in the communication. In another word, authentication has to ensure message integrity and attaches a sender's digital signature along with the message.

Availability

Availability means that we have to ensure network communication works flawlessly without interruption.

VANET is a wireless communication based system and thus it inherits the intrinsic problems associated with wireless networks and networks in gerenal. Some unique challenges that VANETs present include:real time constraits, memory constraints, processing limitations and frequently changing senders. According to Schoch et al. [9], for security reasons, many VANET applications require to use digital signatures, certificates and timestamps to guarantee message integrity, authenticity, and prevent several attacks. However, these benefits also come with significant performance costs.

First, digital signatures and certificates increase network messages' size; thus, they create communication overhead. For example, for each beacon message, even using a compact signature and small key size, e.g. Elliptic Curve Cryptography (ECC), the communication overhead is around 140 bytes (1 digital signature, 1 key, and 1 certificate). At a beaconing rate of 10 Hz and with high vehicle density of 100 vehicles, this translates to approximately 1400 B/s per vehicle node or about 140 kB/s on the communication channel.

Secondly, beside communication overhead, digital signatures and certificates also increase computational overhead. Computational overhead includes signature generation and verification. For example, when a beacon message sent and received, a signature is generated per beacon sent and two signature verifications (sender signature and the certificate authority signature of the certificate) for each beacon received. Assuming of 100 vehicles and a beaconing rate of 10 Hz, this requires verifying around 2000 signatures per second.

Also we can assume that an attacker can send invalid signaturea within a particular communication range. Security attacks like Message modification attack, Denial of Service attack, RSU replication attack and False information attack can be considered as threats to VANET.

IV. Artifical Intelligence for Positioning

An artifical-intelligence system continuosly learns from its past incidents and by its salient feature to discern and recognize its surroundings. Like human beings identify from sounds, images and other sensory inputs, artifical intelligent system recognizes the surrounding environment using the various sensor systems and evalute the next move in a mobile car. Artifical Intelligence can save lives, which makes it the key to greater traffic safety which will bring highly automated driving to our roads. Human computer interface like speech recognition, gesture recognition and camera based machine vision system, RADAR and LIDAR support artifical intelligence and can emulate the function of the human brain. Artifical Intelligence through its deep leaning networks to predict visual represntation of image can predict what will happen next based on object it can detect in the image and what it perceives to be happenig. Any decision making without a clear undersatnding of future trends risk reduced profits or increased losses. An agent is said to behave intelligently when:

a) It has to decide what actions are best for a particular sitution and its end results.

b) It is adaptable to the changing goals and enviornment.

c) It can learn from its past.

When an agent has numerous sensors to gather the information about its surroundings, it can make decision about the exact state of its position and surroundings. In case of VANET, when the communication is taken care by beaconing, a vehicle does not know its exact current and future position and the speed of other vehicles. The only information a vehicle has is the series of beacons transmission rate.

To realize the integration of DSRC and GPS observations, the sensor data fusion logic is a significant issue. The Bayesian filter provides a recursive frame for filtering based data fusion. Considering the computation efficency ina dynamic vehicluar enviornment, the global approaches like Kalman and particle filters for a suboptimal solution to Bayesian filter may suffer from the enormous computational burden, and thus a local approach with pre-defined assumptions to the posterior density is a suitable choice. Among these methods, Kalman and Particle filters are the one's which takes a simpler structure and advanatges in estimation performance over other traditional solutions. Kalman filter is a widely used prediction algorithm. The basic idea behind the prediction algorithms is to estimate guideline to be used as minimum mean square error utilizing the state space model of signal and noise. Kalman filter is a light weight discrete linear estimator that has a recursive property, which means that it improves the state estimate with new measuement through the processing of only the new measurenment and a previous state estimate. Whereas Particle filter, a non linear algorithm, is based on the set of variables and its associated weights. The probablity of a proposition is proportioanl to the weighted porportion of the weights of the particle in which the proposition is true.

Filters have been used along with the packet repletion mode decision algorithm and context adaptive beacon verification method to deliver vehicle position updating data in the method proposed by [14].

V. Authentication with Particle Filter

Message authentication consists of the two fundamental checks: integrity check and identification check. Message authentication must be implemented to allow the vehilces users differentiate reliable information from bogus information. Abeuh and Liu [11] have described the various different solutions to the problem of message authentication in VANET by digitally sigining the messages before sending them. Broadcasting the beacon messages is a strong research area because a significant number of messge transmitted in VANET's are broadcast messages. Significant algorithms are required to minimize broadcast stroms that arise due to packet flooding. Moreover802.11 wireless communication technology is not well suited at handling these transmissions because of frequent retransmissions by vehicles.

This work proposes to augment message authentication with particle filter. A security scheme based on Schoch;s concept called context adaptive beacon verification (CABV) [12] which aims at reducing the computational overhead in validating beacon messages for secured VANET communications. This method requires the verification of signature from initial beacon of new vehicles and from then onwards checking the every nth beacon. To prevent the intermediate spoofed beacons, a linear and non linear estimators are used for future position prediction. If the estimated positions and those recorded in the beacon process varies greatly, then a signature is triggered.

Figure 4 illustrates the working of our Context Adaptive Beacon Verification method along with particle filter. After modeling CABV, We then simulate and test our CABV model through OMNeT++, SUMO and Veins (Initially, we model CABV using MATLAB and later CABV was rewritten in C++ for simulation). Data network simulator are used to simulate the computer networks. They allow researchers to study and evaluate computer networks on different scenarios and settings in a controlled reproducible environment. OMNet++ is a open source, extensible and modular network simulator with GUI and IDE support. Road traffic simulator in VANET simulation aid to produce accurate and valid results for evaluating connected protocols. We have used Vehicles in Network Simulation (Veins)[10] [13] as a middlware that interlinks OMNeT++ and SUMO together by extending each simulator with a dedicated communication module.

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

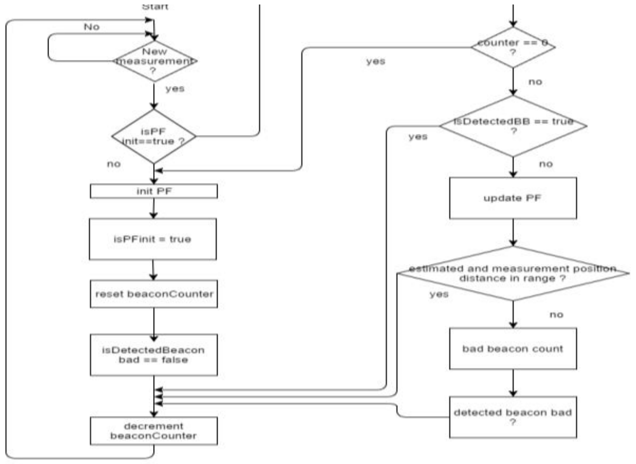

Fig. 4 Flowchart describing working of our CABV method.

Figure 5 shows the flowchart of our working simulated system. The Veins framework includes a comprehensive suite of models to make vehicular network simulations look as real as possible. The GUI and IDE of OMNet++ and SUMO can be used to run simulations. The road traffic simulation is performed by SUMO and a map of the selected area is generated using Openstreet map. Network simulation is performed by OMNet++ along with the physical layer modelling toolkit MiXiM and INET framework, which allows to employ the most precise models of moving and static obstacles by modelling multi-channel multi-technology physical layer in wired and wireless communication. After setting up the system for simulation we use particle filter which was first equated in MATLAB and then converted to C++ to track and predict the future positioning of the vehicle.

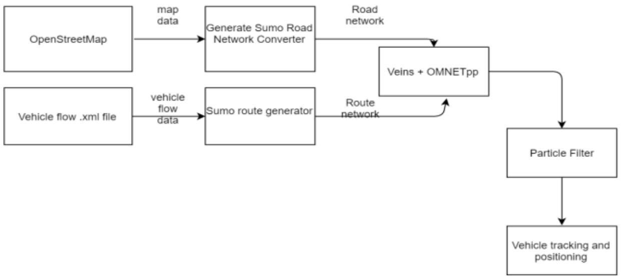

Fig. 5 Flowchart describing working of various simulation tools.

For simplicity and proof of concept, our CABV model uses counters to count total number of beacons received, total number of signature verification performed and number of spoofed beacons that is detected and has signature checked. Our CABV assumes it have signature verification functionality implemented. After collecting all the results, we evaluate the effectiveness of CABV.

VI. Integrate Vehicle and data traffic

We proposed an efficient scheme that uses context adaptive beacon verification along with particle filter (artificial intelligence). With this technique, we could set the system that ensured a low communication overhead and more accurate path prediction when compared with another filter.

Traditional beacon verification method has high overhead; hence when used for VANET's message authentication, it will take a lot of time for compilation. If we go with conventional method, then for around 10-50 cars within the communication range of a vehicle, the vehicle will need to verify around 1000-1500 message per second, which will lead to computational overhead.

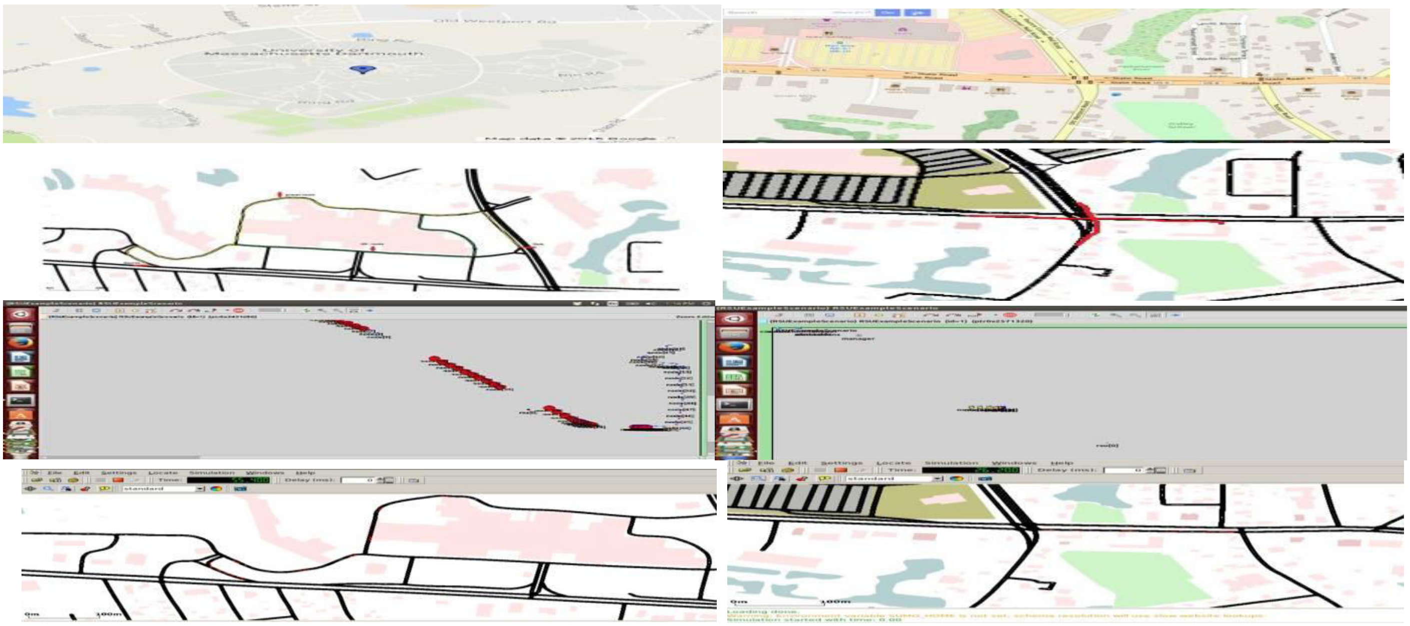

Fig. 6 Simulations of UMassD and State Road (Dartmouth)

To study VANET and to test our CABV method along with particle filter, we created four different scenarios. For simulation purpose, we have chosen OMNeT++ for network simulator, SUMO for traffic simulator and Veins, which acts as a middleware providing IVC simulation model and coordinates operation between OMNet++ and SUMO. Figure 6 captures the SUMO map view and Veins simulation of UMass Dartmouth and State Road (Dartmouth). Each scenario was simulated 15 times to gather enough data for analysis. Yellow and Red trace shows the pre-defined route where the vehicles are simulated with the following characteristics:

1. Acceleration and Deceleration: 2.9 m/s^2 and -5.0 m/s^2
2. Driving imperfection:0.5
3. Min gap between two vehicles: 4.0 m
4. Max Velocity: 16 m/s
5. Car Color: Red

Initial simulation analysis results carried out shows the efficiency of two of the proposed schemes and level of security achieved compared to the case when beacons are signed and verified. Kalman filter along with CABV method perform well when the selected road was linear (UMass D) but when it comes to non-linear path (State Road) with curves and turns, it took couple of seconds to trace back on right path. Whereas particle filter gave exceptional results for both linear and nonlinear paths.

VII. Simulation and Results

Computational Overhead: Our results shows that CABV can save upto 86.5% computational overhead while using Kalman Filter as a prediction validator whereas Particle Filter can save 85.94% computational overhead for the same scenario. With a minor difference of just 0.56%.

Spoofed Beacon Detection: CABV was also able to detect around 76% (24% missed) spoofed beacons with Kalman Filter and 89% (11% missed) spoofed beacons with Particle Filter. The difference turns out to be 13% when it comes to the detection of spoofed beacons.

The model results indicate the significant saving in computational overhead and spoofed beacon detection of our scheme comparing to conventional methods of message verification. The tests result after comparing both filters showed that this methodology can provide accurate vehicle positioning for long distances without using GPS data. The two graphs on the upper side of Figure 7 (a) (b) represents the tracking and future prediction of the vehicles in UMass Dartmouth simulated environment using Kalman and Particle Filter. The 7 (a) figure explains the working Kalman filter which clearly shows the failure of predicting the position when a spoofed message was generated. The system took couple of seconds to regain back to its original position because once the CABV Kalman filter detect the bad beacons it will ignore the remaining beacons of couple of seconds and will not be able to track the position. Where as in Figure 7 (b), the UmassD map is evaluated with Particle filter and the system could track the trajectory positions. The lower two graphs in figure 7 (c) (d) shows the working of Kalman and Particle Filter on State Road Dartmouth. We can see the congestion created in case of Kalman Filter 7 (c) when the vehicles encountered spoofed messages and lost its track completely whereas in case of Particle Filter Fig 7 (d) very less crowding was experienced and the system took around 134 seconds less when compared to Kalman Filter to complete its path.

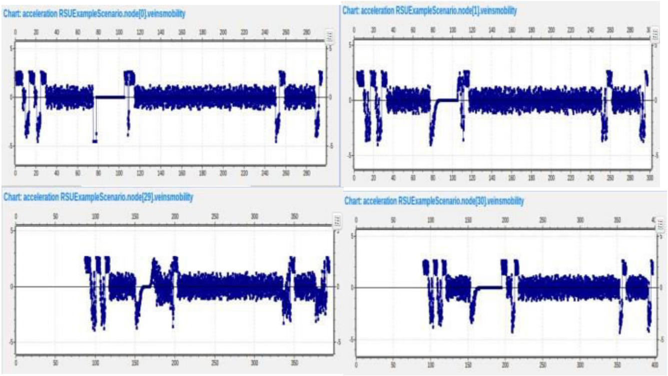

Fig: 7 Kalman vs Particle Filter simulation results on UMassD and State Road (Dartmouth)

VIII. Conclusion and Future Work

This interdisciplinary research shows promising results of applying the artificial intelligence filters to secure the wireless communication of connected vehicles. Particle filter significantly reduces communication overhead while keeping the same detection level of spoofed messages when compared to Kalman filter in VANET applications. We explained that why vehicular networks are important, why networks must be secured and why vehicular networks are promising. Stimulating different scenarios with Context adaptive beacon verification along with Kalman and particle filter on University of Massachusetts Dartmouth and State Road (Dartmouth) proved that it can detect and prevent spoofed attacks and help reducing the computational overhead. But, the Current method of securing the connected vehicle with filters leave the burden of privacy protection on VANET. The practice makes the autonomous cars the target of attack because of the number of spoofed messages missed by context adaptive beacon verification is around 11% (41 out if 46 were detected) which leaves the undetected rate too high to be replaced by conventional verification method.

Future work is planned to quantify the security metrics and omit generations, transmission and verification of signatures and certificates without significant infringement of security. Parameters, such as spoofed message generation and detection will be defined quantitively to reduce the undetected spoofed beacon to an acceptable level. Also, we need to perform extensive testing by assessing the security scheme under various scenarios, thereby reducing the communication overhead and develop an integrated tool for multidisciplinary study of connected vehicles. This work provides the overlook of the system where we had an experimental testbed. This work is planned to be tested in real world to ensure the security and better performance of the vehicles.

ACKNOWLEDGMENT

The authors would like to thank Nhien T Ly for his previous research that led us to this work and his insightful advices to conduct further research.

REFERENCES

[1] B. Vlasic and N. E. Boudette, "Self-Driving Tesla was Involved in Fatal Crash, U.S. Says," Business Day, 30 June 2016. [Online]. Available: https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html?_r=0.

[2] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin and A. Hassan, "Vehicular Ad Hoc Networks (VANETS): Status, Results and Challenges.," *Telecommunication Systems ,* vol. 50, no. 4, pp. 217-241, August 2012.

[3] M. Raya and J. P. Hubaux, "The Security of Vehicular ad hoc networks.," in *3rd ACM workshop on Security of ad hoc and sensor networks.*, Alexandria, VA, USA., 2005.

[4] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur and A. Iyer, "Flooding-Resilient Broadcast Authentication for VANETs," in *17th annual international conference on Mobile computing networking*, New York, 2011.

[5] E. Schoch and F. Kargl, "On efficiency of secure beaconing in VANETs," in *3rd ACM conference on Wireless network security*, Hoboken, New Jersey, USA, March 2010.

[6] S. Eichler, C. Schroth, T. Kosch and M. Strassberger, "Strategies for Context-Adaptive Message Dissemination in Vehicular Ad Hoc Networks.," in *IEEE*, 17-21 July 2006.

[7] Y. J. Abueh and H. Liu, "Message Authentication in Driverless Cars," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 2016.

[8] F. Kargl, E. Schoch, B. Wiedersheim and T. Leinmuller, "Secure and efficient beaconing for vehicular networks," in *5TH ACM International Workshop on Vehicular Inter-Networking*, San Francisco, California, USA, 2008.

[9] F. Gustafsson, F. Gunnarsson, N. Bergman, U. Forssell, J. Jansson, R. Karlsson and P. J. Nordlund, "Particle Filters for Positioning, Navigation and Tracking.," in *IEEE Transactions on Signal Processing*, 2002.

[10] M. Booysen, "Simulating VANET and ITS (using SUMO and OMNET++)," Seminar at UniRC, 2012.

[11] L. D. Ambroggi, "Artifical Intelligence Systems for Autonomous Driving On the Rise," IHS Markit, 13 June 2016. [Online]. Available: https://technology.ihs.com/579746/artificial-intelligence-systems-for-autonomous-driving-on-the-rise-ihs-says.

[12] L. Needhi, S. Bhushan and M. Mahajan, "Intelligent Hazard Routing for VANETs with Point of Interest Evaluation Technique," *International Journal of Computer Science and Mobile Computing,* vol. 4, no. 7, pp. 116-121, 2015.

978-1-5090-6356-7/17/$31.00 ©2017 IEEE