

SECURED ROADWAY WIRELESS COMMUNICATION FOR VEHICLES USING AI TECHNOLOGY

¹Dr. G. MENAKA, M.Sc, M.Phil (CS), Ph.D, ²Dr. C. SHANKAR,

¹ PROFESSOR OF CS CUM VICE PRINCIPAL,

VIVEKANANDHA COLLEGE OF ARTS AND SCIENCES FOR WOMEN(AUTONOMOUS),
 TIRUCHENGODE, TAMILNADU, INDIA menaka.guru@gmail.com

²AP/CIVIL,
 COIMBATORE INSTITUTE OF TECHNOLOGY, COIMBATORE, TAMILNADU, INDIA
shankar.c@cit.edu.in

DOI: <https://doi.org/10.63001/tbs.2025.v20.i01.pp805-814>

KEYWORDS

Distributed denial of service (DoS), VANET, location and monitoring, message authentication, signature verification, wireless communication.

Article Info

Received: 30.01.2025
 Accepted: 18.03.2025
 Published: 28.03.2025

Abstract

In this research work makes use of synthetic intelligence technology for the comfy Roadway wireless communications for AI based vehicles. The vehicular exchange of protection messages (VANET) facilitated via the advert-hoc community. This AI generation will cause independent cars for stopping collisions. The analytical and discriminating capabilities of AI era are constantly being stepped forward as a result of being aware of its surroundings. This capacity is essential for comparing the sincerity and dependability of safety messages for laptop-pushed motors. Presenting fake metre readings, disabling the brakes and other unauthorized controls via sending fake alerts into the VANET, and safety threats. As a powerful defence in opposition to cyber-attacks, counter measures ought to be considered early within the layout process, in preference to afterthought fixes. But contemporary requirements miss security measures like verifying each message sent and obtained via related automobiles, beginning the VANET as much as denial-of-service (DoS) attacks. This interdisciplinary educational research examines the instant wherein message authentication and (DoS) mitigation are balanced, making protection protocols feasible for the deployment of linked cars within the real global. In an effort to reduce transmission and computation complexity, AI filters are used at the side of context-adaptive Signature Verification for message authentication. Combining the data network OMNET++SUMO, a simulation of visitors on the roads, and Veins, an open source VANET simulation framework, the research compares AI filter out performance under extraordinary assaulting situations. The findings influence a green layout selection for securing automobiles with connectivity can talk wirelessly.

I. Introduction

In everyday growing area of vehicular automation, the IOT based totally thoughts are improved related to the connectivity of automobiles. The great use of sensors, which generate tremendous massive records, transforms automobiles as cellular structures for a endless quantity of services and programs. In keeping with a latest projection by using business Insider Intelligence, 10 million related cars can be on the road by using 2020. Generation companies grab a extensive bite of the pie, as evidenced with the

aid of Google's open dedication to the Self-riding automobile challenge and Apple's enigmatic iCar scheme. Startups within the self-sufficient car quarter, like Tesla, ecologically sound electric vehicles. Additionally, suppliers create turnkey answers for manufacturers to include into their vehicles, inclusive of Delphi automobile and Mobileye. As a part of the assessment session for "checking out, Deployment, and improvement of Self-using motors in Massachusetts" at April 27, 2016,

Massachusetts branch of Transportation and the govt office of Housing and monetary improvement made a formidable announcement to assist the kingdom as national fleet of driverless automobiles. By means of relieving people of the want to power, related motors have an impact on society. The country wide highway traffic safety administration estimates that every year, over 43,000 human beings die in motor vehicle accidents inside the use.

But whilst computers perform vehicles, security poses serious problems. 2015 brought the shocking revelation that hackers had remotely taken manipulate of the country. The driver is a connected magazine reporter who works with security researchers Charlie Miller and Chris Valasek to reveal how prone present-day motors. Unfortunately, a pc mistakes cost Tesla an employee in 2016 even as they were trying out their self-using car. This have a look at investigates how nicely related automobile communications can be secured the usage of artificial intelligence (AI). AI device profits expertise from experience so that you can continuously improve its cognitive cognizance of its surroundings and to speedy attain clever conclusions. Particularly, message spoofing and denial-of-carrier (DoS) assaults are made extra vulnerable through the deployment of the Vehicular ad-hoc community (VANET) by connected motors. This newsletter indicates Bayes-primarily based AI forecasting algorithms like Kalman and Particle Swarm To stumble on faked messages and be resilient to DoS attacks filter further to well-known

filters. The security system provides a context-adaptive signature verification approach that notably reduces the computational overhead in certifying safety alerts by means of utilizing the functions unique to surface transit. The selective beacon message validation defence in opposition to DoS attacks does no longer lessen the efficacy of faulty message detection. The results make certain comfy verbal exchange among cars and infrastructures. (V2V).

II. CONNECTED VEHICLE STRUCTURE

Vehicular ad-hoc community (VANET), a well-known era that uses shifting automobiles as verbal exchange nodes to form an advert hoc community, permits vehicles to communicate to one another wirelessly. Routers that are deployed in strategic places alongside the direction assure non-stop vehicle radio coverage, probably encircling the complete metropolis. The related automobile VANET structure permits possible to allow automobiles and/or networking gadget to "talk" to each other. Motors with On-Board devices (OBU) mounted can communicate with one another. Street-aspect devices (RSU) growth verbal exchange insurance even as delivering rapid statistics quotes. A dedicated short-variety verbal exchange (DSRC) frequency has been allotted for VANET. So that you can keep away from collisions, related motors may be used inside the destiny with cars without onboard processors through the usage of sensors like Radio Detection and Detection and varying (LIDAR) and RADAR.

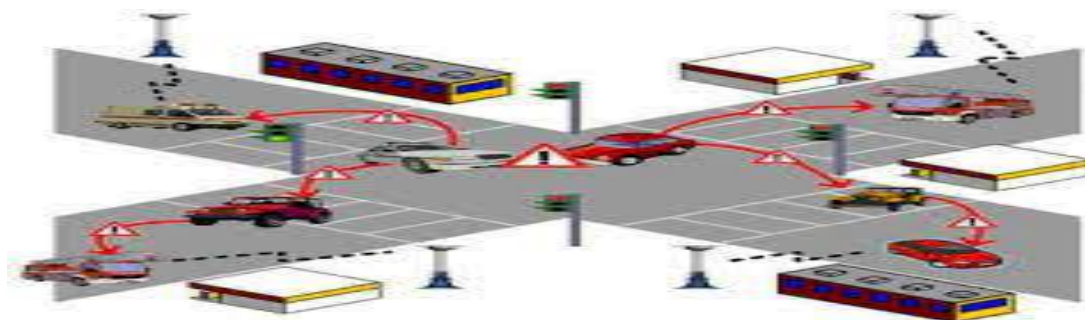
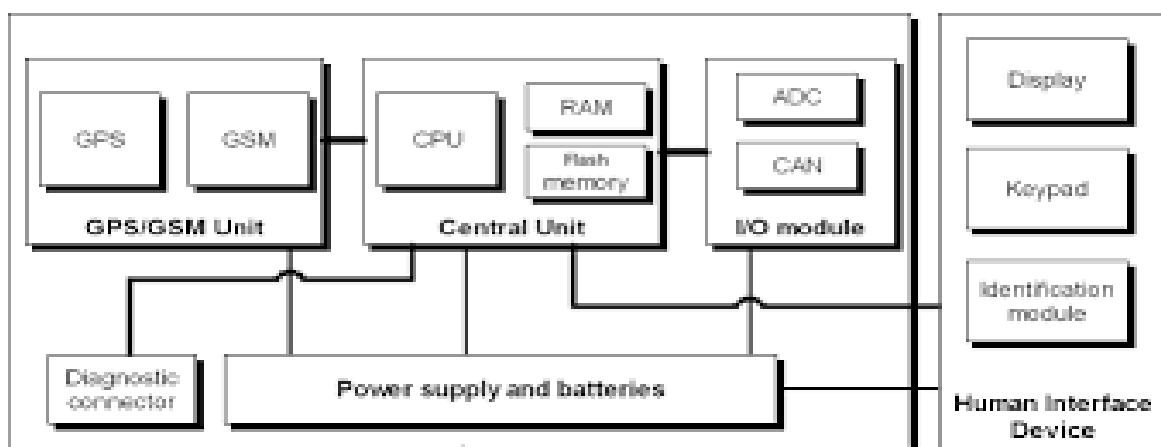


Fig 1. Roadway Vehicular Adhoc Network (VANET)

An on-board tool is built on WAVE requirements consisting of IEEE 802.11p, IEEE1609 (IEEE 1609.2, IEEE 1609.3, IEEE 1609.Four, and IEEE 1609.Eleven), and SAE J273. (OBU). It's miles a committed pc with networking hardware and sensors that improves management of updated on-board diagnostics (OBD-II). Since the middle of the Nineteen Nineties, OBD-IIs have been required in all cars. They provide electronic approach for controlling engine operations, tracking chassis and accessories, along with emissions, and diagnosing vehicle troubles. An instance of a standard OBU without OBD-II The components of this gadget are the manage unit, the transmission subsystem, and the sensor community. The embedded platform for industrial computing (EPIC) single-board

commercial pc serves as the idea for the management and communicate unit. The significant control Unit serves because the device's beating coronary heart. The usage of GPS to permit vicinity-dependent cooperative services, the unit and the sensors provide one-manner conversation, that's crucial for positioning, pace, and time. The GSM unit permits each car-to-car and vehicle-to-infrastructure mobile wi-fi verbal exchange because it is a -way gadget. To hold music of the interest of all nearby motors, the principal manipulate unit of OBU methods and decrypts the statistics from the higher layer and saves it in flash memory. The GPS module transmits the vehicle's location, pace, and acceleration numerous times in keeping with 2nd thru records sharing.

**Fig 2. On Board Unit (OBU)**

The selection and Judgment making a block ensures that an awesome preference can be made to make sure the safety, preventing assaults from impostor drivers. The module that communicates with the passenger inside the car is referred to as the human system interface. LEDs and a built-in buzzer permit the consumer recognize how the software is operating and what the OBU's kingdom is. The user is provided with data on site visitors

situations, radio control, map view, emergency or collision warnings, and vehicle pace. The consumer can use a Bluetooth wi-fi connection to switch all the information displayed to his smart cellphone or pill. Packages going for walks on the consumer interface device are in fee of sending caution messages when risks are located. An RSU plays similar responsibilities to an OBU that is stationary. OBU is extra effective and often has a related

hyperlink to the internet backbone. As a way to offer networking infrastructure for stepped forward performance and enforced protection in communications among connected motors, RSUs are regularly put each a hundred–two hundred meters alongside a direction. With records speeds of up to fifty-four Mbps, modern-day IEEE 802.11a compliant devices can aid wireless communications amongst moving motors.

However, whilst traditional IEEE 802.11 MAC protocols are utilized in automobile contexts, variable speeds, dynamic traffic, and environmental regulations result in big overheads. In order to efficiently manage V2V and V2I communications, the US Federal Communications Commission has allocated 75MHz of freely licenced spectrum in the 5.9GHz band for Dedicated Short-Range Communication (DSRC) in VANET. A DSRC module's communication range is constrained to maximum diameter of 1 km. The available data transfer rates are 3, 4.5, 6, 9, and 12 Mbps for vehicle speeds between 60 and 120 km/h and 9, 12, 18, 24, and 27 Mbps for vehicle speeds between 0 and 60 km/h. It makes use of BPSK, QPSK, and 16-QAM. According to IEEE STD 802.11-2007, the modulating mode might be QAM or 64-QAM. The regional DSRC standards developed by the US were renamed to the world standards under IEEE 802.11p Wireless Access in Vehicular Environment as the ASTM 2313 working group for DSRC shifted to the IEEE 802.11 standard group. (WAVE).

The top application layer standard in the Internet Protocol Stack is WAVE IEEE 1609.1, which specifies protocols for both safety applications like brake activations and non-safety applications like traffic guidance. Because topological restrictions imposed by roads call for more straightforward routing algorithms, the Transport Layer and Network Layer are closely connected. They are grouped together under IEEE 1609.3, where WAVE Management Entity (WME) serves as the management plane and WAVE Share Message Protocol (WSMP) serves as the operating plane conventional IP and TCP/UDP for network and transport, respectively. The Logical Link Control Layer (LLC) and traditional IEEE 802.11 Lower Media Access Control Layer are linked by IEEE 1609.4 Upper Media Access Control Layer (UMAC), which is how the Data Link Layer (DLL) handles the complexity of communications in moving vehicles. Data Link Layer's management Entity (MXME) and Lower Media Access Control (LMAC) Layer Management Entity are both found on the management plane (LME). The Physical Layer utilizes the IEEE 802.11a WAVE Physical Layer, and the Physical Layer administration Entity (PLME) uses it for administration. The two Physical Layer protocols and the two lower media protocols at the Data Link Layer are collectively referred to as IEEE 802.11p. All layer tiers of security are addressed by IEEE 1609.2.

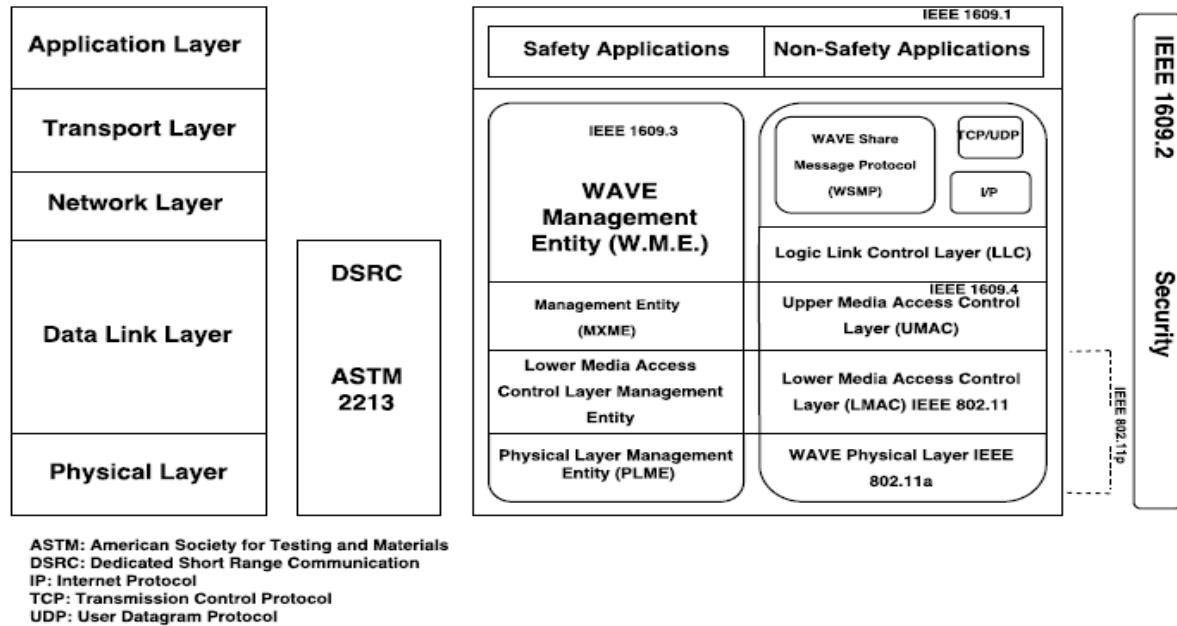


Fig 3. The internet protocol stack's VANET

III. COMPUTER-CONNECTED VEHICLES: SECURITY ISSUES

As their entire life is linked to situations wherein people's lives are in risk, connected automobiles' security is extremely crucial. It's miles essential that a malicious man or woman does now not adjust the records or the utility. As a way to set up the driver's legal responsibility, the privacy must be preserved. The system must be truthful sufficient to no longer divulge essential facts to inaccurate assets. As an example, a dishonest driver would possibly send fake reports of a traffic jam or an coincidence on a favored street to convince different automobiles to keep away from taking that course, or they might break into the automobile's pc system to make it do something they need. Cars should handiest be moving on the street in shrewd transportation networks as properly. Naive broadcasting and shrewd broadcasting are the two fundamental methods of inter-car communications. A vehicular network model, an attacker version, and a few assault methods are all defined in via Raya et al. They provide an expansion of answers, together with nameless public keys, tamper-evidence hardware, and digital signatures. The prevailing VANET broadcast

authentication trendy, that is susceptible to signature flooding, is attempted to be constant. An incident referred to as "signature flooding" causes sufferers' computing competencies to end up overloaded with excessive signature verification requests. Their look at indicates authentication structures that may counter assaults involving signature flooding. The existence threading safety difficulty, however, continues to be an trouble today and is receiving fairly little interest.

The networks for connected vehicles can use the conventional list of security requirements for computer networking, which is as follows:

Confidentiality (Privacy)

Only the intended recipient and the sender are able to understand conveyed messages thanks to confidentiality or privacy.

Message reliability

In order to maintain message integrity, the data being sent between the sender and the recipient must stay intact during transmission.

If we are unable to ensure that, we must be able to recognize altered communications.

Authorization at the endpoint

With end-point authentication, each party to the communication can be identified by the sender and the receiver. To put it another way, authentication must guarantee message integrity and include the digital signature of the sender.

Availability

We need to make sure community connection runs easily and without hiccups with a purpose to preserve availability.

The VANET inherits the issues that emerge evidently with wi-fi networks and networks in general due to the fact it's far primarily based on wi-fi verbal exchange. Some of the particular demanding situations that VANETs bring encompass real-time troubles, memory constraints, processing boundaries, and often changing senders. Consistent with Schoch with a view to ensure message integrity, authenticity, and to thwart diverse assaults, many VANET programs are required to use virtual signatures, certificates, and timestamps. These advantages are accompanied via vast performance charges, although.

First, network messages end up larger as a result of virtual signatures and certificates, which upload to conversation overhead. As an instance, the communication overhead for every beacon message is approximately 140 bytes, even when using a short signature and tiny key size, inclusive of Elliptic Curve Cryptography (ECC). With a high vehicle density of 100 vehicles and a beaconing price of 10 Hz, this equates to more or less 1400 B/s in step with vehicle node or more or less one hundred forty kB/s at the verbal exchange channel.

2nd, similarly to transmission fees, digital signatures and certificates raise computational charges. Computational waste includes the

procedure of making and verifying signatures. For example, every time a beacon message is despatched and obtained, signature verifications—the sender's signature and the certificates authority's signature—are produced. This calls for confirming about 2000 signatures consistent with second, assuming one hundred cars and a ten Hz beaconing price. Moreover, we are able to suppose that within a selected conversation variety, an attacker can send invalid signatures. Threats to VANET consist of security assaults along with the Message change assault, Denial of provider assault, RSU Replication assault, and false information assault.

IV. ARTIFICIAL INSIGHT FOR POSITIONING

A machine learning system continuously learns new abilities through analyzing its environment and trying to draw from its previous errors. An artificially intelligent system can recognize its environment by using a diverse range of sensor systems, much like how humans recognize objects based on noises, sights, and other sense information. A s well as determine what is best for a moving vehicle. Since it has the potential to save lives, artificial intelligence (AI) is the key to enhanced road safety and the initiation of highly autonomous driving. Speech recognition, gesture recognition, camera-based machine vision systems, RADAR, and LIDAR are some examples of human computer interfaces that support artificial intelligence and can simulate brain function. In artificial Intelligence the deep learning methodology will help to predict how a picture will appear. Depending on the elements it can make out in the picture and what it interprets as taking place. Any decision made without a thorough knowledge of possible future trends runs the risk of producing lower profits or higher losses. When an agent behaves intelligently.

a) It must decide the best course of action in considering the situation and the expected outcomes.

b) It can change depending on the situation and the objectives.

c) It is capable of picking up lessons from the past.

An agent can determine the exact state of its location and surroundings when it has a large number of sensors to gather data about them. A vehicle cannot know its exact present and future positions when communicating in a VANET via beaconing. The only information a vehicle has is the rate at which a series of beacons are transmitting. The integration of DSRC and GPS observations is significantly hampered by the sensor data fusion logic. A recursive framework for data fusion based on filtering is provided by bayesian analysis. Given the computing effectiveness in a dynamic vehicle environment, a local technique using pre-defined assumptions about the posterior density is a good alternative to global approaches like Kalman and particle filters for a suboptimal solution to Bayesian filters. The simplest of these methods, Kalman and particle filters, perform better at estimating performance than more traditional methods. In that, the Kalman filter is a very popular prediction algorithm. The main concept of the prediction algorithms is to estimate a guideline that will be used as the minimal mean square error. This one is done using the state space model of signal and noise. The Kalman filter, a recursive discrete linear estimator with low computational complexity, uses new measurements to improve an earlier state estimate by only processing the new measurement. The non-linear particle filter algorithm, in contrast, is based on a number of variables and the weights assigned to them. The probability that a statement is true is determined by the weighted ratio of the particle's weights. To deliver vehicle position updating data, filters have been used in addition to the packet

repletion mode decision technique and the context adaptive beacon verification method proposed by [14].

V. PARTICLE FILTER AUTHENTICATION

The identification check and the integrity check are the two vital checks used for message authentication. Message authentication must be implemented in order to give vehicle users the ability to distinguish between reliable information and false information. Abeuh and Liu have presented several options for handling the problem of message authentication in VANET, including digitally signing messages before sending them. Context-adaptive beacon verification (CABV), a technique that aims to reduce the computational burden associated with validating for secure VANET connections and beacon messages, is a security strategy based on the concept put forth by Schoch. It is necessary for this method to verify the signature of the initial beacon of new cars and examining the every nth one after that beacon. There is a need for important algorithms to reduce broadcast storms brought on by packet flooding. Additionally, 802.11 wireless communication technology is not well suited to handle the repeated transmissions caused by automobiles. In this work, a particle filter is suggested as a way to increase message authentication security. We demonstrate our Context Adaptive Beacon Verification approach and particle filter. First, we modelled CABV in MATLAB, and then we modified CABV in C++ for simulation. Following CABV modelling, we use OMNeT++, SUMO, and Veins to simulate and validate our CABV model. Data network simulators allow for the simulation of computer networks. They enable researchers to examine and evaluate computer networks in a regulated, repeatable setting under a variety of conditions and circumstances. The road traffic simulator used in the VANET simulation aids in producing reliable result for analysing connected

protocols. A middleware we used to link OMNeT++ and SUMO is referred to as a vehicle in network simulation (Veins). It shows the flowchart for our operational simulated system. To build the most realistic-looking vehicular network simulations possible, the Veins framework comes with a full range of different models. The OMNeT++ GUI and IDE of SUMO can be used to run simulations. The chosen area is mapped using Open Street Map, while SUMO simulates the movement of traffic on the roads. The most precise models of moving and stationary objects can be used with the INET framework, OMNeT++, and physical layer modelling tools Maxim by simulating the multi-channel, multi-technology physical layer in wired and wireless communication. In order to track and predict the future location of the vehicle, we use a particle filter that was equalized in MATLAB and then converted to C++ after the system was set up for simulation. For simplicity and proof-of-concept, our CABV model uses counters to keep track of the total number of beacons received, the total number of signature checks finished, and the total number of fake beacons found and their signatures verified. Our CABV anticipates having capabilities for signature verification in place. After gathering all the information, we evaluate the CABV's effectiveness.

VI. INCLUDE DATA TRAFFIC FROM VEHICLES

We propose a practical approach that combines the particle filter of artificial intelligence with context-adaptive beacon verification. In comparison to another filter, we were able to design a system using this technique that ensured minimal communication overhead and more accurate path prediction. It will take a long time to compile the traditional beacon verification method when used for VANET message authentication because it has a large overhead. The conventional method adds computational overhead because the vehicle must verify between 1000 and 1500 messages per second

for each car within 10 to 50 feet of it. To investigate VANET and assess our CABV strategy when combined with a particle filter, we created four unique scenarios. In order to simulate, we have chosen OMNeT++ as the network simulator, SUMO as the traffic simulator, and Veins as the middleware that provides the IVC simulation model and controls the communication between the two. Figure 6 shows the UMass Dartmouth and State Road SUMO map view and Veins simulation (Dartmouth). Each situation was approximated 15 times in order to gather sufficient data for analysis. The simulated vehicles follow the pre-planned route, which is highlighted in yellow and red on the trace.

1. A speed difference of -5.0 m/s² and an acceleration of 2.9 m/s²
2. Roadway recklessness: 0.5
3. A minimum of 4.0 metres must separate each car.
4. The top speed is 16 m/s.
5. Car colour red.

Preliminary simulation study results illustrate the efficacy of two of the proposed systems and the level of security attained in comparison to the case where beacons are signed and confirmed. The Kalman filter and CABV approach work well when the chosen road is linear (UMass D). It takes a few seconds to retrace your steps on the right path, though, when the chosen road (State Road) is not linear and has bends and turns. The results from the particle filter, on the flip hand, were excellent for both linear and nonlinear pathways.

VII.SIMULATION AND OUTCOMES

Computational Overhead:

According to our findings, CABV may reduce computational overhead by up to 86.5% when Kalman Filter is used as a prediction validated,

while Particle Filter can reduce computational overhead by up to 85.94% in the same situation. with a negligible variation of 0.56%. Spoofed Beacon Detection: Using the Kalman and Particle filters, respectively, CABV was also able to detect about 76% (24% missed) and 89% (11% missed) of spoofed beacons. When it comes to the detection of fake beacons, the difference turns out to be 13%. The model findings show that, as compared to traditional techniques of message verification, our scheme significantly reduces computational overhead and can detect spoofed beacons. The experiments' results, which included a comparison of both filters, revealed that this technology can deliver precise Long-distance vehicle placement without using GPS data.

- (a) (Top)'s two graphs show the tracking and future prediction of the cars in a simulated environment created by UMass Dartmouth using Kalman and Particle Filter. The functioning Kalman filter is which also illustrates the evident inability to anticipate the position when a faked message was created. The system needed a few seconds to return to its previous position since the CABV Kalman filter ignores any further beacons after detecting a defective beacon, making it impossible to track the system's position.
- (b) Uses a particle filter to evaluate the UMassD map so that the system can track locations on a trajectory.
- (c) (Lower)'s two graphs demonstrate the operation of the Kalman and Particle Filters on State Road. Dartmouth. When the vehicles met faked messages and lost all track, we can observe the congestion that was caused by the Kalman filter in In contrast, the Particle filter experienced very little crowding and took 134 seconds less to complete its trip.

VIII. CONCLUSION AND FUTURE WORK

In this interdisciplinary study, the use of artificial intelligence filters to secure the wireless connection of connected vehicles has yielded encouraging results. Particle filter significantly reduces communication costs while maintaining the same level of faked message detection when compared to Kalman filter in VANET applications. The importance of automotive networks, the requirement for network security, and the potential of vehicular networks were all covered. The University of Massachusetts Dartmouth and State Road (Dartmouth) simulations of various scenarios showed its ability to detect and prevent spoofing attacks while also assisting in the reduction of computational overhead. Context adaptive beacon verification, Kalman analysis, and particle filtering were used. However, the current method of securing connected vehicles with filters places the burden of privacy protection on VANET. Autonomous vehicles become a target for attack as results of the widespread use of faked messages that context cannot detect. Since only 41 of the 46 adaptive beacons were found, the verification rate for adaptive beacons is only about 11%, making the undetected rate too high to be replaced by conventional verification techniques. The formation, transmission, and verification of certificates and signatures will be excluded in future work in order to quantify security metrics and avoid significantly compromising security. Quantitative definitions of factors like the creation and detection of spoofed messages will be made in order to reduce the number of undiscovered spoofed beacons to a manageable number. Additionally, we must develop a platform that is integrated for multidisciplinary research on connected cars and carry out extensive testing by analyzing the security infrastructure under various circumstances. This solution offers an overview of the architecture that was the premise for our experimental analysis. This

effort will be put to the test in real-world scenarios to ensure the security, safety and quality of car travelling method.

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/selfdriving-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. Booyesen, "Simulating VANET and ITS (using SUMO and OMNET++)," Seminar at UniRC, 2012.
- [11] L. D. Ambroggi, "Artificial Intelligence Systems for Autonomous Driving On the Rise," *IHS Markit*, 13 June 2016. [Online]. Available: <https://technology.ihs.com/579746/artificial-intelligence-systems-forautonomous-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.