IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Security in Wireless Communication of Connected Vehicles against attacks using Artificial Intelligence

Dr. T. Prem Chander
Associate Professor & Head of the Department, AI & ML Department,
Neil Gogte Engineering College.

Abstract: This work applies artificial intelligence(AI) to secure wireless dispatches of Connected Vehicles. Vehicular Ad- hoc Network(VANET) facilitates exchange of safety dispatches for collision avoidance, leading to tone- driving buses . An AI system continuously learns to compound its capability in sapient and feting its surroundings. similar capability plays a vital part in assessing the authenticity and integrity of safety dispatches for buses driven by computers. Falsification of cadence readings, disablement of boscage function, and other unauthorized controls by spoofed dispatches fitted into VANET crop as security pitfalls. Countermeasures must be considered at design stage, as opposed to afterthought patches, effectively againstcyber-attacks. still, current norms oversubscribe security measures by validating every communication circulating among Connected Vehicles, making VANET subject to denial- of- service(DoS) Attacks. This interdisciplinary exploration shows promising results by searching the pivot point to balance between communication authentication and DoS forestallment, making security measures practical for the real- world deployment of Connected Vehicles. Communication authentication adopts environment- Adaptive hand Verification strategy, applying AI pollutants to reduce both communication and calculation outflow. Combining OMNET, a data network simulator, and SUMO, a road business simulator, with modes, an open source frame for VANET simulation, the study evaluates AI pollutants comparatively under colorful attacking scripts. The results lead to an effective design choice of securing wireless dispatches for Connected Vehicles.

Keywords — Adaptability to denial- of- service(DoS) attacks, artificial intelligence(AI) for stoked cognitive capability, Connected Vehicles, Vehicular Ad- hoc Network(VANET), position and shadowing, communication authentication, hand verification, wireless communication

INTRODUCTION

The Internet of effects makes buses more connected in moment's burgeoning technology of vehicular robotization. The proliferation of detectors that collect huge quantities of data transforms buses into mobile platforms for endless operations and services. Connected Vehicles are getting reality with ten million hitting the road in 2020, estimated by Business Insider Intelligence lately. Technology companies take a big piece from the pie, similar as Google's public commitment to tone- Driving Car Project and Apple's mysterious strategy on iCar. Startups request for driverless buses , including Tesla on environmental-friendly electric motors. In addition, suppliers, like Delphi Automotive and Mobileye, develop turnkey systems for automakers to make into their vehicles. Massachusetts Department of Transportation, along with the Executive Office of Housing and Economic Development, made a bold advertisement, at the harkening Session for " Testing, Deployment, and Development of tone- Driving Vehicles in Massachusetts " on 27 April 2016, to promote the state the Testbed of Driverless Vehicles for the nation.

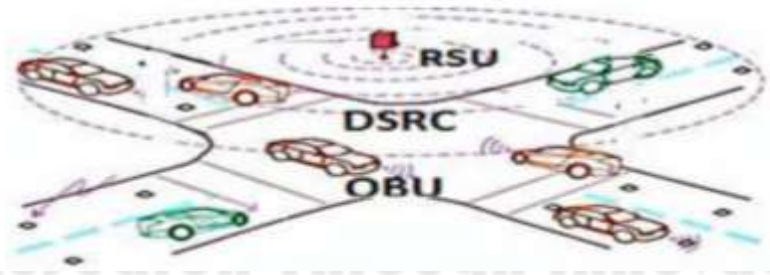
Connected Vehicles impact the society by releasing mortal from driving. According to the National Highway Traffic Safety Administration, over thirty thousand people die in motor vehicle accidents in the United States alone every time . When buses driven by computers, still, security posts significant challenges. In 2015, a news shocked the nation that hackers ever took control of a Jeep and killed its machine in stir on the trace(1). The situation isn't as dire as it sounds the motorist is a Wired magazine journalist working with security experimenters Charlie Miller and Chris Valasek to show the vulnerability of ultramodern vehicles. sorely, in 2016, Tesla lost an hand while testing its tone- driving auto due to computer malfunction

This work explores the effectiveness of artificial intelligence(AI) in securing dispatches among Connected Vehicles. An AI system learns from experience to compound its cognitive capability about its terrain continuously and to make good opinions presently(3). Vehicular Ad- hoc Network(VANET) stationed by Connected Vehicles expands security vulnerability inherited from wireless dispatches, particularly in communication spoofing and denial- of- service(DoS) attacks. This paper proposes AI prophetic algorithms grounded on Bayes proposition like Kalman and flyspeck Sludge along with general pollutants to descry spoofed dispatches with adaptability to DoS attacks. exercising the features unique to face transportation, the security scheme adopts environment- adaptive hand verification strategy, significantly reducing the computational outflow in authenticating safety dispatches. picky confirmation of lamp dispatches protects VANET against DoS attacks without losing the effectiveness of defective communication discovery. The results insure secure dispatches for vehicles to vehicles(V2V) and vehicles to architectures V2I)

ARCHITECTURE OF CONNECTED VEHICLES

Vehicles connect to each other wirerlessly with Vehicular Ad- hoc Network(VANET), a trending technology that takes moving buses as communication bumps to form a spontanous network. Routers, strategically placed along the road, insure constant content for vehicular dispatches, conceivably blanketing an entire megacity(4).Fig. 1 illustrates the armature of Connected Vehicles with VANET, where buses " talk " to each other and/ or the networking infrustructure. On- Board Units OBU) equipped on vehicles enable buses to communicate. Road- Side Units(RSU) expand dispatches with both spacial content and high data speed. A spetrum of devoted Short- Range Communication(DSRC) is assigned for VANET. previous to request penetration, Connected Vehicles also work with buses of no OBUs being equipped via detectors, similar as RAdio Discovery And Ranging(RADAR) and LIght Discovery And Ranging(LIDAR), to avoid collisions

Detection And Ranging (RADAR) and LIght Detection And Ranging (LIDAR), to avoid collisions.

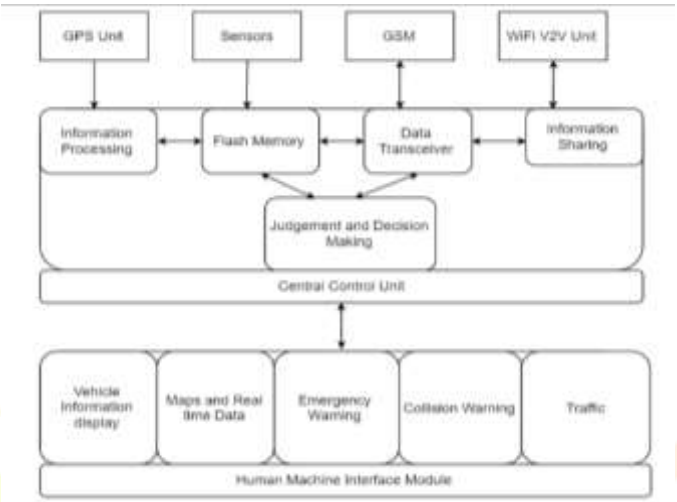


Vehicular Ad-hoc Network (VANET)

An On- Board Unit(OBU) is grounded on WAVE norms including IEEE802.11 p, IEEE1609(IEEE1609.2, IEEE , IEEE1609.4, IEEE1609.11) and SAE J273. It's a special purpose computer with communication bias and detectors, accelerating control of streamlined On- Board Diagnostics (OBD- II). OBD- IIs, mendentory in motors sincemid-90s, give electronic means to control machine functions, cover lattice and accessories including emigration, and diagnose auto problems.Fig. 2 shows a schematic illustration of a typical OBU banning OBD- II. It consists of the control unit, the communication

subsystem and the detector network. Control and communication unit is grounded on the single board artificial PC of EPIC form(Bedded Platform for Industrial Computing)

The Central Control Unit acts as a heart of the whole system. The GPS unit and the detectors provides one-way communication which is necessary positioning, haste and time, to enable position dependent united services. The GSM unit is a two- way communication which ensures the mobile wireless communication among vehicle to vehicle and vehicle to structure communication. The Central Control unit of OBU process and decipher the information from upper subcaste and save it in flash memory to keep a track of all the neighboring vehicles geste. Information participating broadcasts the vehicles position, speed and acceleration several times per second, which is got from GPS module.



On-Board Unit (OBU)

The Judgement and Decision Making block ensures to make a wise decision to insure the security hence avoiding the attacks by false motorists. mortal Machine Interface is the module which interact with the person sitting inside the auto. LED's and a figure in buzzer provides operation feedback to the stoner and inform the status of the OBU. Information regarding vehicle speed, radio control, chart view, exigency or collision warnings and business status is being participated with the stoner. stoner can get all the details displayed to his smartphone or a tablet via Bluetooth wirelesslink.However, also advising If any hazard isencountered.messages are being transferred and controlled by operation running on the stoner interface device.

A Road- Side Unit(RSU) functions like a stationary OBU powered by further computing coffers and frequently with a wired connection to the Internet backbone. RSUs are generally installed at every 100-200 measures along a road to give networking structure for enhanced performance and enforced security in dispatches among Connected Vehicles.

Being IEEE802.11 a biddable bias with data rates of up to 54 Mbps can support wireless dispatches among moving buses . still, varying pets, dynamic traffics, and environmental constraints induce heavy charges when traditional IEEE802.11 MAC protocols operate in vehicular scripts. To support V2V and V2I dispatches efficiently, the US Federal Dispatches Commission has assigned 75 MHz of freely certified diapason in the5.9 GHz band for devoted Short Range Communication(DSRC) in VANET. The communication area covered by a DSRC module is limited to the outside of 1Km periphery. The data transmission rates can be 9, 12, 18, 24, and 27 Mbps for 0 – km/ h vehicle haste and 3,4.5, 6, 9, and 12 Mbps for 60 – km/ h vehicle haste. The system uses BPSK, QPSK, 16- QAM, or 64- QAM as the modulating mode(IEEE STD802.11- 2007).

The indigenous norms of DSRC by US is renamed to the transnational norms under IEEE802.11 p Wireless Access in Vehicular Environemnt(WAVE) as the ASTM 2313 working group for DSRC migrated to the IEEE802.11 standard group. 3 depicts WAVE(5) in the Internet Protocol mound. At the top operation Layer, IEEE1609.1 defines protocols for both Safety operations similar as boscage activations andNon-Safety operations like business 411

. The Transport Subcaste and Network Layer are tightly coupled because topological constraints by roads warrant simpler routing algorithms. They are lumped into IEEE1609.3 with WAVE Management Entity WME) as a operation aeroplane and WAVE Share Message Protocol(WSMP) as an operation aeroplane compatible to traditional TCP/ UDP for transport and IP for network. The Data Link Subcaste deals with the complexity of moving vehicle dispatches with peak and conquer IEEE1609.4 Upper Media Access Control Layer(UMAC) links between Logical Link Control Layer(LLC) and traditional IEEE802.11 Lower Media Access Control Layer(LMAC). On the operation aeroplane , Data Link Layer contains operation reality(MXME) and Lower Media Acess Control Layer Management Entity(L-MLME). The Physical Subcaste uses IEEE802.11 a WAVE Physical Layer for operation and Physical Layer Management Entity(PLME) for operation. The two protocols at the Physical Subcaste and the two lower media protocols at the Data Link Layer are inclusively called IEEE802.11p. Security is addressed across all the layers by IEEE1609.2.

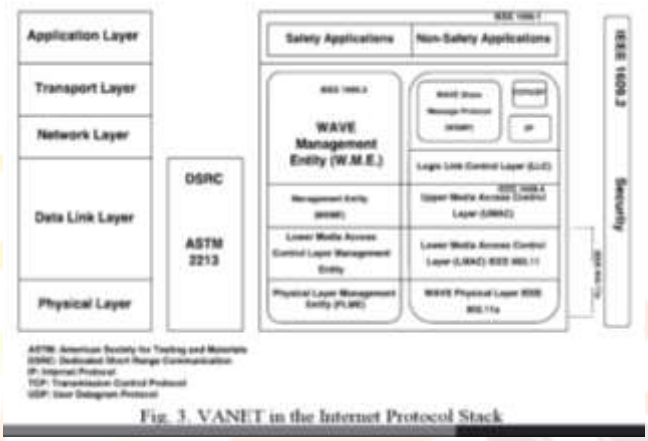


Fig. 3. VANET in the Internet Protocol Stack

SECURITY CHALLENGES IN CONNCECTED VEHICLES

The security of Connected Vehicles plays a vital part as their very actuality relates to life threating situtions. It is important that the information or the program should not modified by the mallicious person. The sequestration must be maintained similar that the liablity of the motorist is determined. The system should be dependable enough similar that it does n't partake the important information with the false sources. For illustration, a vicious motorist can shoot a false information of business jam or accident on a asked road to encourage other buses to avoid that route or by playing the auto system and make them work as the way they want. Also, in intelligent transportation systems, vehicles need only be with exertion on the road. There are substantially two types of inter vehicle dispatches naïve broadcasting and intelligent broadcasting(6)

In(7), Raya etal. describe a vehicular network model, an bushwhacker model and a many attack types. They give numerous results,e.g. digital autographs, tamper- evidence device, crucial operation, and anonymous public keys. Hsiao et.al.(8) try to break the current VANET broadcast authentication standard that is vulnerable in hand flooding. hand flooding is an event that inordinate hand verification requests that exhause the computational coffers of victims. Their paper propose two authentication schemes that can alleviate hand flooding attacks. still, till now the life threading security issue still persist and veritably little attention is paid on it. The following classical list of security conditions in computer networking can be applied to connected vehicles networks

Confidentiality (Privacy)

Confidentiality or sequestration ensures that only the sender and intended receiver comprehend transmitted communication.

Message integrity

Communication integrity requires the transmitted data between the sender and receiver is unchanged in transmission for whatever , we need to be suitable to If we can not guaranteethat.detect modified dispatches.

End-point authentication

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

Availability

Vacuity means that we've to insure network communication works faultlessly without interruption. VANET is a wireless communication grounded system and therefore it inherits the natural problems associated with wireless networks and networks in gerenal. Some unique challenges that VANETs present includereal time constraits, memory constraints, recycling limitations and constantly changing senders. According to Schoch etal.(9), for security reasons, numerous VANET operations bear to use digital autographs, instruments and timestamps to guarantee communication integrity, authenticity, and help several attacks. still, these benefits also come with significant performance costs.

First, digital autographs and instruments increase network dispatches' size; therefore, they produce communication outflow. For illustration, for each lamp communication, indeed using a compact hand and small crucial size,e.g. Elliptic wind Cryptography ECC), the communication outflow is around 140 bytes(1 digital hand, 1 key, and 1 instrument). At a beaconing rate of 10 Hz and with high vehicle viscosity of 100 vehicles, this translates to roughly 1400 B/ s per vehicle knot or about 140 kB/ s on the communication channel.

Secondly, beside communication outflow, digital autographs and instruments also increase computational outflow. Computational outflow includes hand generation and verification. For illustration, when a lamp communication transferred and entered, a hand is generated per lamp transferred and two hand verifications(sender hand and the instrument authority hand of the instrument) for each lamp entered. Assuming of 100 vehicles and a beaconing rate of 10 Hz, this requires vindicating around 2000 autographs per second.

Also we can assume that an bushwhacker can shoot invalid signaturea within a particular communication range. Security attacks like Communication revision attack, Denial of Service attack, RSU replication attack and False information attack can be considered as pitfalls to VANET.

ARTIFICAL INTELLIGENCE FOR POSITIONING

An artifical- intelligence system continuosly learns from its once incidents and by its salient point to discern and fete its surroundings. Like mortal beings identify from sounds, images and other sensitive inputs, artifical intelligent system recognizes the girding terrain using the colorful detector systems and evalute the coming move in a mobile auto. Artifical Intelligence can save lives, which makes it the key to lesser business safety which will bring largely automated driving to our roads. mortal computer interface like speech recognition, gesture recognition and camera grounded machine vision system, RADAR and LIDAR support artifical intelligence and can emulate the function of the mortal brain. Artifical Intelligence through its deep leaning networks to prognosticate visual represntation of image can prognosticate what will be next grounded on object it can descry in the image and what it perceives to be happenig. Any decision making without a clear undersatnding of unborn trends threat reduced gains or increased losses. An agent is said to bear intelligently when

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

b) It's adaptable to the changing pretensions and enviornment.

c) It can learn from its once

When an agent has multitudinous detectors 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 irradiating, a vehicle doesn't know its exact current and unborn position and the speed of other vehicles. The only information a vehicle has is the series of lights transmission rate

To realize the integration of DSRC and GPS compliances, the detector data emulsion sense is a significant issue. The Bayesian sludge provides a recursive frame for filtering grounded data emulsion. Considering the calculation efficency ina dynamic vehicluar enviornment, the global approaches like Kalman and flyspeck pollutants for a sour result to Bayesian sludge may suffer from the enormous computational burden, and therefore a original approach withpre-defined hypotheticals to the posterior viscosity is a suitable choice. Among these styles, Kalman and flyspeck pollutants are the bone's which takes a simpler structure and advanatges in estimation performance over other traditional results. Kalman sludge is a extensively used vaticination algorithm. The introductory idea behind the vaticination algorithms is to estimate guideline to be used as minimal mean square error exercising the state space model of signal and noise. Kalman sludge is a light weight separate direct 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 former state estimate. Whereas flyspeck sludge, a non direct algorithm, is grounded 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 flyspeck in which the proposition is true.

Pollutants have been used along with the packet starvation mode decision algorithm and environment adaptive lamp verification system to deliver vehicle position streamlining data in the system proposed by(14).

AUTHENTICATION WITH PARTICLE FILTER

Communication authentication consists of the two abecedarian checks integrity check and identification check. Communication authentication must be enforced to allow the vehilces druggies separate dependable information from bogus information. Abeuh and Liu(11) have described the colorful different results to the problem of communication authentication in VANET by digitally sigining the dispatches before transferring them. Broadcasting the lamp dispatches is a strong exploration area because a significant number of messge transmitted in VANET's are broadcast dispatches. Significant algorithms are needed to minimize broadcast stroms that arise due to packet flooding. also802.11 wireless communication technology is not well suited at handling these transmissions because of frequent retransmissions by vehicles.

This work proposes to compound communication authentication with flyspeck sludge. A security scheme grounded on Schoch; s conception called environment adaptive lamp verification(CABV)(12) which points at reducing the computational outflow in validating lamp dispatches for secured VANET dispatches. This system requires the verification of hand from original lamp of new vehicles and from also onwards checking the every nth lamp. To help the intermediate spoofed lights, a direct and non direct estimators are used for unborn position vaticination. If the estimated positions and those recorded in the lamp process varies greatly, also a hand is touched off.

Figure 4 illustrates the working of our Context Adaptive Beacon Verification system along with flyspeck sludge. After modeling CABV, We also pretend and test our CABV model through OMNeT, SUMO and modes(originally, we model CABV using MATLAB and latterly CABV was rewritten in C for simulation). Data network simulator are used to pretend the computer networks. They allow experimenters to study and estimate computer networks on different scripts and settings in a controlled reproducible terrain. OMNet is a open source, extensible and modular network simulator with GUI and IDE support. Road business simulator in VANET simulation aid to produce accurate and valid results for assessing connected protocols. We've used Vehicles in Network Simulation(modes)(10)(13) as a middlware that interlinks OMNeT and SUMO together by extending each simulator with a devoted communication module.

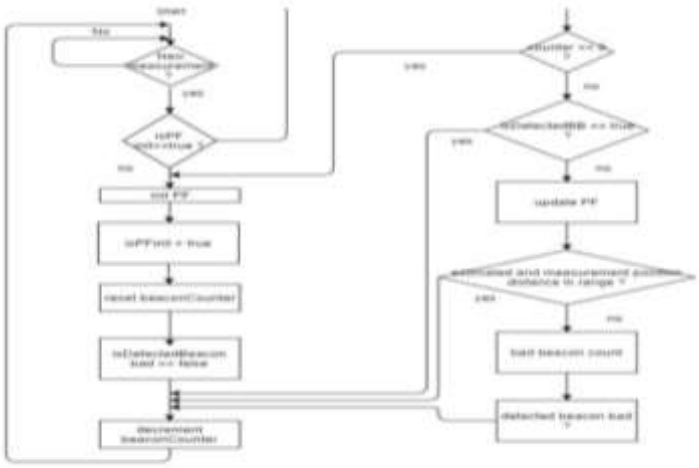


Fig. 4 Flowchart describing working of our CABV method.

Figure 5 shows the flowchart of our working dissembled system. The modes frame 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 business simulation is performed by SUMO and a chart of the named area is generated using Openstreet chart. Network simulation is performed by OMNet along with the physical subcast modelling toolkit MiXiM and INET frame, which allows to employ the most precise models of moving and static obstacles by modellingmulti-channelmulti-technology physical subcaste in wired and wireless communication. After setting up the system for simulation we use flyspeck sludge which was first equated in MATLAB and also converted to C to track and prognosticate the unborn positioning of the vehicle.

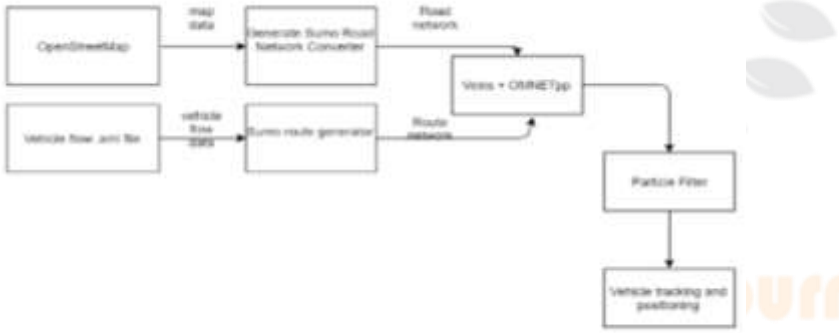


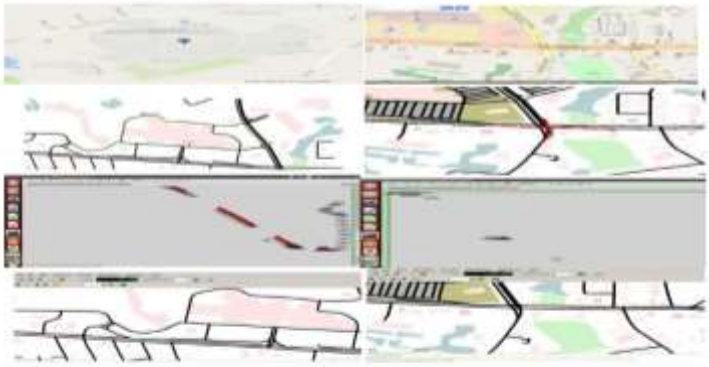
Fig. 5 Flowchart describing working of various simulation tools.

For simplicity and evidence of conception, our CABV model uses counters to count total number of lights entered, total number of hand verification performed and number of spoofed lights that's detected and has hand checked. Our CABV assumes it have hand verification functionality enforced. After collecting all the results, we estimate the effectiveness of CABV.

INTEGRATE VEHICLE AND DATA TRAFFIC

We proposed an effective scheme that uses environment adaptive lamp verification along with flyspeck sludge(artificial intelligence). With this fashion, we could set the system that assured a low communication outflow and more accurate path vaticination when compared with another sludge

Traditional Lamp verification system has high above; hence when used for VANET's communication authentication, it will take a lot of time for compendium. If we go with conventional system, also for around 10- 50 buses within the communication range of a vehicle, the vehicle will need to corroborate around 1000- communication per second, which will lead to computational above.



To study VANET and to test our CABV system along with flyspeck sludge, we created four different scripts. For simulation purpose, we've chosen OMNeT for network simulator, SUMO for business simulator and modes, which acts as a middleware furnishing IVC simulation model and coordinates operation between OMNet and SUMO. Figure 6 captures the SUMO chart view and modes simulation of UMass Dartmouth and State Road(Dartmouth). Each script was dissembled 15 times to gather enough data for analysis. unheroic and Red trace shows thepre-defined route where the vehicles are dissembled with the following characteristics

1. Acceleration and retardation2.9 m/ s2 and-5.0 m/ s2

2. Driving fault0.5

3. Min gap between two vehicles4.0 m

4. Max Velocity 16 m/ s

5. Auto Color Red

Original simulation analysis results carried out shows the effectiveness of two of the proposed schemes and position of security achieved compared to the case when lights are inked and vindicated. Kalman sludge along with CABV system perform well when the named road was direct(UMass D) but when it comes tonon-linear path(State Road) with angles and turns, it took couple of seconds to trace back on right path. Whereas flyspeck sludge gave exceptional results for both direct and nonlinear paths.

SIMULATION AND RESULTS

Computational Outflow Our results shows that CABV can save upto86.5 computational outflow while using Kalman Filter as a vaticination validator whereas flyspeck Sludge can save85.94 computational outflow for the same script. With a minor difference of just0.56

Caricatured Beacon Detection CABV was also suitable to descry around 76(24 missed) caricatured lights with Kalman Filter and 89(11 missed) caricatured lights with flyspeck Sludge. The difference turns out to be 13 when it comes to the discovery of spoofed lights.

he model results indicate the significant saving in computational outflow and caricatured lamp discovery of our scheme comparing to conventional styles of communication verification. The tests affect after comparing both pollutants showed that this methodology can give accurate vehicle positioning for long distances without using GPS data. The two graphs on the upper side of Figure 7(a)(b) represents the shadowing and unborn vaticination of the vehicles in UMass Dartmouth simulated terrain using Kalman and flyspeck Sludge. The 7(a) figure explains the working Kalman sludge which easily shows the failure of prognosticating the position when a caricatured communication was generated. The system took couple of seconds to recapture back to its original position because once the CABV Kalman sludge descry the bad lights it'll ignore the remaining lights of

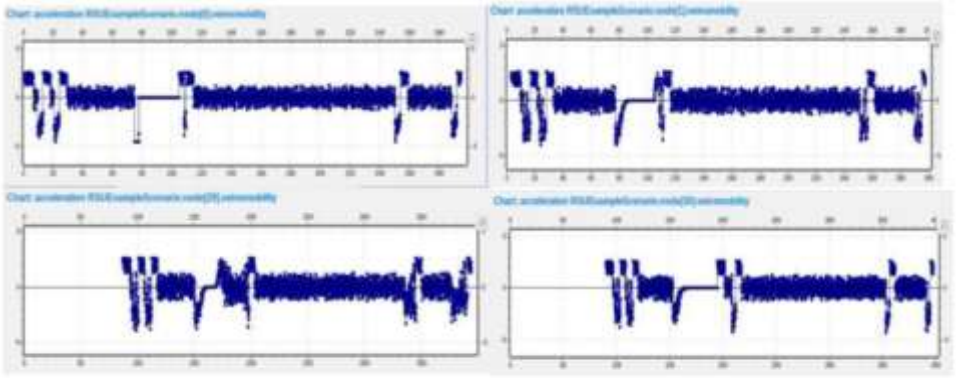


Fig: 7 Kalman vs Particle Filter simulation results on UMassD and State Road

couple of seconds and won't be suitable to track the position. Where as in Figure 7(b), the UmassD chart is estimated with flyspeck sludge and the system could track thetrajectory 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 traffic created in case of Kalman Filter 7(c) when the vehicles encountered caricatured dispatches and lost its track fully whereas in case of flyspeck Sludge Fig 7(d) veritably less crowding was endured and the system took around 134 seconds less when compared to Kalman Filter to complete its path.

CONCLUSION AND FUTURE WORK

This interdisciplinary exploration shows promising results of applying the artificial intelligence pollutants to secure the wireless communication of connected vehicles. flyspeck sludge significantly reduces communication outflow while keeping the same discovery position of spoofed dispatches when compared to Kalman sludge in VANET operations. We explained that why vehicular networks are important, why networks must be secured and why vehicular networks are promising. Stimulating different scripts with environment adaptive lamp verification along with Kalman and flyspeck sludge on University of Massachusetts Dartmouth and State Road(Dartmouth) proved that it can descry and help spoofed attacks and help reducing the computational outflow. But, the Current system of securing the connected vehicle with pollutants leave the burden of sequestration protection on VANET. The practice makes the independent buses the target of attack because of the number of spoofed dispatches missed by environment adaptive lamp verification is around 11(41 out if 46 were detected) which leaves the undetected rate too high to be replaced by conventional verification system.

Unborn work is planned to quantify the security criteria and forget generations, transmission and verification of autographs and instruments without significant violation of security. Parameters, similar as spoofed communication generation and discovery will be defined quantitively to reduce the undetected caricatured lamp to an respectable position. Also, we need to perform expansive testing by assessing the security scheme under colorful scripts, thereby reducing the communication outflow and develop an intertwined 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 insure the security and better performance of the vehicles.

REFERENCES

(1)B. Vlasic andN.E. Boudette," tone- 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 andA. Hassan," Vehicular announcement Hoc Networks(VANETS) Status, Results andChallenges.," Telecommunication Systems,vol. 50,no. 4,pp. 217- 241, August .

(3)M. Raya andJ.P. Hubaux," The Security of Vehicular ad hoc networks.," in 3rd ACM factory on Security of ad hoc and detector networks., Alexandria, VA,USA., 2005.

(4)H.-C. Hsiao,A. Studer,C. Chen,A. Perrig,F. Bai,B. Bellur andA. Iyer," Flooding-flexible Broadcast Authentication for VANETs," in th annunal transnational conference on Mobile calculating networking, New York, 2011.

(5)E. Schoch andF. Kargl," On effectiveness 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 andM. Strassberger," Strategies for environment- Adaptive Communication Dispersion in Vehicular Ad Hoc ," in IEEE, 17- 21 July 2006.

(7)Y.J. Abueh andH. Liu," Communication Authentication in Driverless buses," in 2016 IEEE Symposium on Technologies for Homeland Security HST), 2016.

(8)F. Kargl,E. Schoch,B. Wiedersheim andT. Leinmuller," Secure and effective beaconing for vehicular networks," in 5TH ACM International Workshop on VehicularInter-Networking, San Francisco, California, USA, 2008.

(9)F. Gustafsson,F. Gunnarsson,N. Bergman,U. Forssell,J. Jansson,R. Karlsson andP.J. Nordlund," flyspeck Pollutants for Positioning, Navigation andTracking.," in IEEE Deals on Signal Processing, 2002.

(10)M. Booysen," bluffing VANET and ITS(using SUMO and OMNET)," forum 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 andM. Mahajan," Intelligent Hazard Routing for VANETs with Point of Interest Evaluation fashion," International Journal of Computer Science and Mobile Computing, vol. 4,no. 7,pp. 116- 121, 2015. View cantina