Authenticating Communication of Autonomous Vehicles With Artificial Intelligence

Neetha George[1] **and Jeena Thomas**[2]

1 P G Scholar, Department of Computer Science and Engineering, St.Joseph's College of Engineering and Technology, Palai, Kerala, India.
2 Assistant Professor,Department of Computer Science and Engineering, St.Joseph's College of Engineering and Technology, Palai, Kerala, India.

E-mail: neethageorge06@gmail.com

E-mail: jeena.thomas@sjcetpalai.ac.in

Abstract. Autonomous vehicles in Vehicular Ad-hoc Networks(VANET)-the spontaneous creation of a wireless network for data exchange to the domain of vehicles may pave the way for future systems where computers take over the art of driving. It aids in transferring secure messages for proper communication between the vehicles. Unauthorized access like injecting spoofed messages to VANET can arise as an extreme threat. So remedies should be taken at early degree of architectonic process.Denial-of Service(DoS) attack takes place while validating each message in VANET ,so an equity between message authentication and DoS prevention should be maintained.This paper discusses on diverse security demanding situations and distinct techniques to secure message transfer between the vehicles that are connected wirelessly.
Keywords-Artificial Intelligence,Vehicular Ad-hoc Network(VANET),wireless communication,message authentication, security issues

1. Introduction

The Internet of Things (IOT)[1][2],is one of the most flourishing technology which makes vehicles connected each other. It connects devices, machines and tools to the internet by means of wireless technologies. VANET[3][4] is a type of network in which the interaction of vehicles occur by exchanging messages between them. The safe exchange of messages can lead to collision avoidance, traffic congestion control, thus ensuring the driver a smooth driving experience. But there can be also many attacks faced by VANET[5] like monitoring attacks, social attacks, timing attacks, application attacks, and network attacks. So the connected vehicles should be secured properly. There are several existing methods for securing them.

Regarding the colossal gains expected from vehicular communications and massive vehicles(hundreds of millions worldwide), it is understood that the intra-communication of vehicles can turn into the greatest admissible recognition of mobile ad hoc networks.GPS acceptors in addition to communication capabilities,which are the most suitable assimilation of on-board computers and spotting devices, open immense trading chances, hence boosts astounding research challenges. One of the major issues is security; very little attention has been dedicated untill now to the safety of vehicles in the network. Probably, the size of the network, the speed of the vehicles, the relevance of their geographic location, the very intermittent interconnection, and the inevitable gradual distribution of effective resources shape the threat very peculiar and challenging.

2. Overview of VANET

2.1. Architecture of VANET

Vehicles are connected to each other wirelessly with Vehicular Ad-hoc Network (VANET)[5], an advanced technology that takes moving cars as communication nodes to form a instinctive network. Routers, deliberately placed along the road, insure constant coverage for vehicular communications. VANET. Vehicles communicate to each other with On-Board Units(OBU) rigged on vehicles. Road-Side Units (RSU) expand communications with both geographical inclusion and tremendous speed of data.Dedicated Short-Range Communication (DSRC)[6][7] - a two way wireless communication that is short- to- medium-range ensures enormous transmission of data crucial in communications-based valid security functions is entrusted for VANETs. Vehicles also work with OBUs armed with sensors, such as RAdio Detection And Ranging (RADAR) and LIght Detection And Ranging (LIDAR), to avoid collisions.

The Central Control Unit acts as a heart of the whole system. The GPS[8] unit and the sensors provides one-way communication which is necessary positioning, velocity and time, to empower interdependent services which are position based. 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[11] works on and decode the data from top layer and store it in flash memory to record all the neighbouring vehicles behaviour. Information Sharing broadcasts the position of vehicles, their acceleration and speed several times per second, which is got from GPS module[9]

The Judgement and Decision Making block facilitates to take an appropriate decision to assure the protection thereby averting the intrusions by false drivers. Information regarding vehicle speed, radio control, map view, emergency or collision warnings and traffic status is being shared with the user. User can get entire details displayed to his smartphone or a tablet via Bluetooth wireless link. The alerting messages are being sent and controlled by application running on the user interface device when any risk is encountered. A Road-Side Unit (RSU)[10][11] works as a static OBU powered by more computing properties and have frequent wired connection to the Internet that is considered to be the backbone. RSUs are usually installed at each 100-200 meters across a road to provide networking infrastructure for enhanced performance and enforced security in transmitting messages in vehicular network.Figure 1 illustrates various components of an On-Board Unit.

2.2. Security Attacks in VANET

VANET security has evolved to be a major concern in the society. All the current stations should be authenticated before they contact the available services in the network. The attack enlists the process of identification which represents the whole network to serious aftereffects. In a Vehicular network the authentication safeguards to protect the secured nodes from the outside or inside attackers who tricks the network using a fake identification.The securing scheme process will take place whenever a vehicle tends to link to the network or any service.

Attacks on confidentiality will be a key security mechanism in VANET communications, which ensures the data should accessed by authorized user. within the absence of mechanism, the VANET have to ensure the exchanged message confidentiality, while it's far drastically prone to assaults. Attacks on availability is a most crucial role in VANET which assure the network has been an functional one and also offer needed information during functioning time. Attacks on authentication and identification has emerged as an important discussion in security of VANET. All the actual stations need to be secured in the network before they come in association with the available services. The attack employs the process of identification which represents the

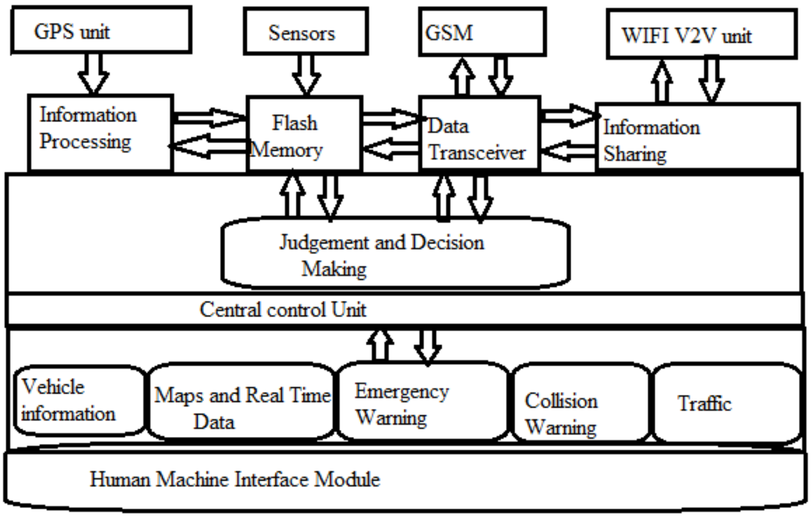

Figure 1. On-Board Unit

whole network to serious consequences. Whenever a vehicle tends to link to the network or any service, the authentication process will takes place. Attacks on integrity and data trust in a vehicle has to ensure that swapped data should not been amended during transmission. These mechanisms aids to safeguard information against deletion, alteration or supplementary attack. Attacks on non-repudiation means, the ability to endorse that the provider and the acceptor are the individuals who can send and receive the messages. The non-abrogation of data origin establish that the information is send to respective sender and the non-repudiation of advent have to make sure that data has been received only authenticated receiver.[12]

3. Authentication Mechanisms in VANET

3.1. Authentication with Digital Signatures

Authentication with Digital Signatures[13][14] is one the excellent techniques for securing the VANET messages since they sign each of the messages before passing them to the acceptor side.It uses a Public key Infrastructure(PKI) to provide security due to huge number of individuals in the network.Each of the vehicle in the network will be contributed with a pair of public/private key.A private key signs the message before it is transferred and includes Certification Authority(CA)certificate.A tamper-proof device along with private keys is necessary in each vehicle where the confidential messages are tracked and out-gone data are signed. Little time later, the sender simulcasts the key and instructs all that this revealed key is not to be used in the future. Receivers cache the actual message until the key is received and then verify the signature.Symmetric cryptographic primitives are used by this verification.Digital signature working is shown in figure 2

Digital Signatures provide speed,security,authenticity,tracking,improper prevention facilities. The existing broadcast authentication standard of Digital Signatures in VANETs is susceptible to signature flooding.Here the excessive signature verification requests exhaust the computable functions of targets. To overcome this challenge of Digital signatures, two efficient broadcast authentication schemes, Fast Authentication (FastAuth) and Selective Authentication (SelAuth) can be used.

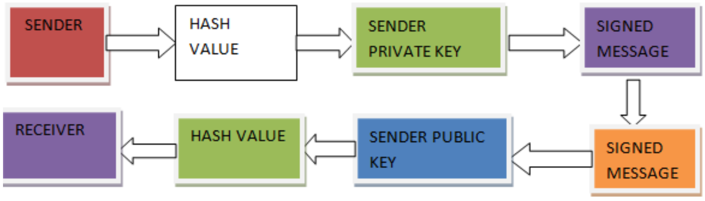

Figure 2. Authentication with Digital Signature

3.2. Authentication with Fast Authentication scheme

FastAuth,is an adequate One-Time Signature(OTS) scheme to secure beacon messages. The innovation in FastAuth[15] is the layout of a sequential Huffman Hash Tree (CHT),which provides the predictability in vehicle mobility to generate small signatures. Every beacon has to be checked when they are received because the beacon may contain definitive and crucial safety information. The recent VANET signature standard is computationally costly, but traditional OTS provides instant verification with increased communication overhead.Inspired by this exclusive challenge,the target of FastAuth is to gain fast authentication with short signatures.

Each vehicle in FastAuth divides its timeline into a sequence of prediction intervals at higher levels. In each prediction interval, a vehicle performs three steps: Beacon Prediction, Key Pair Construction, and Signature Broadcast. In Beacon Prediction at the starting of a prediction interval, all vehicles forcast their beacon messages for the next I beacons. For this vehicles use the probability distribution of the distance vector between two successive beacons based on data of the past trajectory.In Key Pair Construction before transferring any beacon message in this interval, the vehicle needs to build an OTS public key and one interval worth of OTS private keys. A chained Huffman hash tree (CHT), links these pre-computed keys together in a fashion that reduces the size of signatures and generates a single public key.In Signature Broadcast after beacon prediction and construction of the key, a vehicle signs its OTS public key using ECDSA signatures and then simulcasts this ECDSA signed public key PKots along with the first beacon in this prediction interval. Moreover, to retain a high beacon update frequency during severe packet loss, we assimilate Forward Error Correction into FastAuth to recover missed beacons.[16]

3.3. Authentication With Selective Authentication Scheme

To overcome the challenge for creating a decisive verification scheme for multi-hop applications, SelAuth[15], a signature verification protocol which can quickly block the escalation of invalid signatures without verifying all receiving signatures at every hop can be effectively used. In particular, SelAuth uses neighbor identification to avoid enactment and per neighbor verification probability, adjusted dynamically as wrong signatures are received, to achieve isolation. Neighbors of a vehicle communicates directly with the vehicle. L SelAuth also uses warning pushback to accelerate the desolation of pernicious vehicles. As in many other probabilistic verification schemes, vehicles running SelAuth verify an incoming message with a certain probability in order to help identify invalid signatures.However, an important difference is that in preceding work such a probability depends entirely on the local status of the receiver, disregarding where this message is from or whether other vehicles have checked this message. SelAuth leverages ancillary information shared between neighbours to facilitate the probability adjustment for fast and efficient isolation.

The core components of SelAuth are forwarder identification and warning pushback.This enables SelAuth to concentrate faster than other probabilistic verification schemes and be more resource-efficient than the Verify-All approach. Forwarder (or neighbor) identification enables the receiver of a message to effectively find which of its neighbors sent or forwarded this message. In SelAuth, vehicles detecting an invalid signature will initiate a Complaint message to warn vehicles at the previous hop.It is referred to be the Pushback message as it is pushed towards the producer.

4. Securing autonomous vehicles With Artificial Intelligence

An artificial-intelligence system continuously learns from its past incidents and by its pertinent feature to discern and recognize its surroundings. It can think like humans and can save lives,thus improve traffic safety and autonomous driving. An agent is said to behave intelligently when has to decide what actions are best for a particular situation and its end results. It is adaptable to the changing goals and environment and can learn from its past.[19]

4.1. Artificial Intelligence For Positioning

With the help of sensors which collects the information about its environment,agents can take decision about the correct state of its locations and surroundings . In case of VANET, when the communication is guided by beaconing,[17] a vehicle is unaware about its actual and upcoming location and other vehicles speed. The single data available to a vehicle is the sequential transfer rate of the beacons. To realize the assimilation of DSRC and GPS findings, the sensor data fusion logic is a serious issue. Considering the computation efficiency in a dynamic vehicular environment, the widely used techniques like Kalman and particle filters[18] for a sub optimal solution to Bayesian filter may suffer from the collusive computational burden, and thus a local approach with pre-defined assumptions to the posterior density is a suitable choice[20]

4.1.1. Authentication With Particle Filter Two basic checks are provided by Message Authentication: integrity check and identification check. Message authentication is to differentiate the malicious vehicles from the valid ones Broadcasting the beacon messages is one of the relevant research area because an effective number of message transmitted in VANETs are broadcast messages. Significant algorithms are required to more reduce broadcast storms which emerges due to packet flooding. To integrate message authentication with particle filter there is a security scheme based on Schoch;s concept called context adaptive beacon verification (CABV)[18] which aims at decrementing the computational overhead in authenticating beacon messages for protected vehicular message transfer. Here to validate the signatures each initial to the n beacons coming from vehicles are verified . To avoid the in-between intruded beacons, a linear and non linear estimators are taken for upcoming location forecast. If the predicted positions and that are tracked in the beacon works change immensely, then a signature is provoked.

5. Modified Approach of Context Adaptive Beacon Verification Method With Particle Filter

In the modified approach,at first particle filter will track the location of the vehicle and it is initialized with beacon messages.The vehicle will update its current location frequently to the network.The distance of the vehicle tracked from the particle filter is compared with this distance.If there is wide difference,the vehicle considered as malicious one and the beacon counter is incremented.

Figure 3 illustrates the working of the modified approach of Context Adaptive Beacon Verification method along with particle filter.

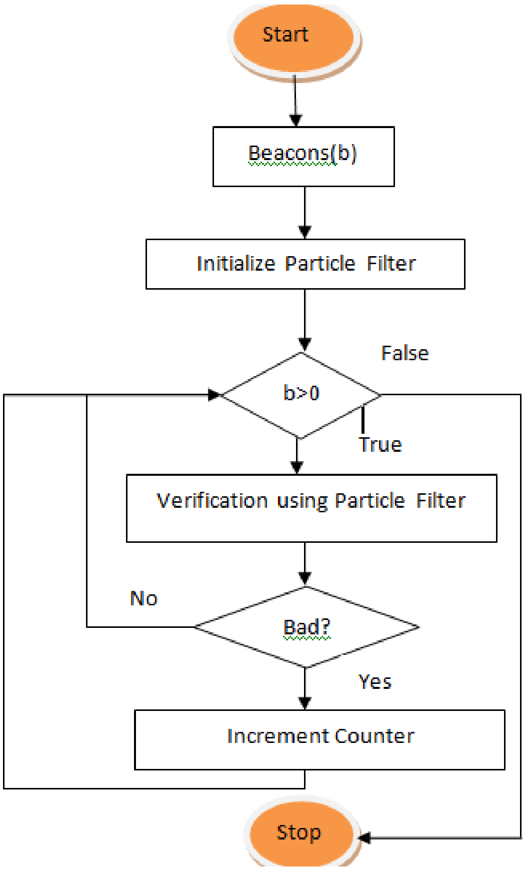
Start
Beacons(b)
Initialize Particle Filter
False
b>0
True
Verification using Particle Filter
No
Bad?
Yes
Increment Counter
Stop

Figure 3. : Modified Approach for Working of CABV method With Particle Filter

6. Conclusion

Since autonomous vehicles are paving a great future to self driving,large amount of vulnerable attacks take place in vehicular networks.This review shows promising results of securing the wireless communication of autonomous vehicles including various methods.We first analyzed Authentication of VANETs with Digital Signatures ,which uses signed messages.Eventhough it secured the network,resulted in computational burden.We later discussed on Fast Authentication and Selective Authentication schemes which were able to overcome some disadvantages of Digital Signatures,but had computational overhead leaving spoofed beacons undetected.Then we saw Particle filter that particularly reduces communication overhead and detection level of spoofed messages will be kept same. Context adaptive beacon verification(CABV) with particle filter proved that it can detect and prevent spoofed attacks and can reduce the computational overhead.But this method also leaves certain number of spoofed beacons undetected.So the study of modified approach of CABV with particle filter is considered in future which can increase the efficiency .The detailed study of further possible vulnerable attacks with this approach will remain for the future scope of development.

7. References

[1] Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., Sarma, S.E.: 2008 The *Internet of Things.* First International Conference, IOT 2008, LNCS 4952, Springer

[2] Shen Subin, Mao Yanqin, Fan Quli, Zongping, Huang Wei. 2010 *Conceptual model and architecture of Internet of Things [J].* Journal Of Nanjing University Of Posts And Telecommunications (Natural Science Edition)

[3] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin and A. Hassan,2012 *Vehicular Ad Hoc Networks (VANETS): Status, Results and Challenges.,*

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

[5] Stampoulis, A. and Chai, Z. (2007). *A survey of security in vehicular networks.*

[6] Bai, F., and Krishnan, H. 2006. Reliability analysis of DSRC *wireless communication for vehicle safety applications.* IEEE intelligent transportation systems conference , Toronto

[7] Kenney J B. 2011 *Dedicated Short-Range Communications (DSRC) Standards in the United States.* Proceedings of the IEEE, Vol. 99(7) pp.

[8] Alfred Leick, John Wiley and Sons, 1995 *The Global Positioning System* GPS Satellite Surveying 2nd Edition,

[9] Thong, S.T.S.; Chua Tien Han; Rahman, T.A., *Intelligent Fleet Management System with Concurrent GPS and GSM Real-Time Positioning Technology,2007.* 7th International Conference on ITS

[10] J. Lee and C. Kim, 2010 *A roadside unit placement scheme for Vehicular Telematics networks,* in AST10

[11] Qiong Yang, Lin Wang, Weiwei Xia, Yi Wu, Lianfeng Shen 2014 International Conference on Connected Vehicles and Expo (ICCVE)

[12] I.A. Sumra, I. Ahmad, H. Hasbullah, J.-L. bin, Ab Manan,2011 *Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET),* in: 3rd International Congress on Ultra Modern Telecommunications and Control Sys- tems and Workshops (ICUMT) IEEE

[13] Igor Furgel and Kerstin Lemke 2004*A review of the digital tachograph system.* In Workshop on Embedded IT-Security in Cars (escar)

[14] Lutz Gollan and Christoph Meinel. 2002*Digital signatures for automobiles.* In Systemics, Cybernetics and Informatics (SCI)

[15] Hsu-Chun Hsiao, Ahren Studer,Chen Chen, Adrian Perrig 2011 *Flooding-Resilient Broadcast Authentication for VANETs* Las Vegas, Nevada, USA.

[16] Kiho Lim, D. Manivannan 2016 *An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks* at Science Direct vehicular communications

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

[18] F. Gustafsson, F. Gunnarsson, N. Bergman, U. Forssell, J. Jansson, R. Karlsson and P. J. Nordlund,2002 *Particle Filters for Positioning, Navigation and Tracking.,* in IEEE Transactions on Signal Processing S. Eichler, C. Schroth, T. Kosch and M. Strassberger,2006 *Strategies for Context-Adaptive Message Dissemination in Vehicular Ad Hoc Networks.,* in IEEE

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

[20] L. D. Ambroggi,2016 *Artifical Intelligence Systems for Autonomous Driving On the Rise*, IHS Markit,Available: https://technology.ihs.com/579746/artificial-intelligence-systems-forautonomous-driving-on-the-rise-ihs-says.