Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

# VEHICULAR COMMUNICATION SECURITY ISSUES RESOLUTION USING VARIOUS MACHINE LEARNING ALGORITHMS

**Ms. Saleha saudagar**, Dept.Of Computer Science Engineering, SAGE University Indore.
**Dr Rekha Ranawat,** Professor, Dept. Of Computer Science Engineering, SAGE University Indore

**Abstract**
The world is moving towards the artificial intelligence; vehicles are no more exceptions to it. Vehicular communication and intelligent transportation system are emerging technology when combined with Machine learning techniques solve various issues. While vehicles moving on the road faces many issues, security is considered as one of the major issues of vehicular communication. In this paper the various aspects of security and its solution using machine learning is identified. Misbehavior detection mechanism used for position falsification mechanism is focused here and its implementation using supervised machine learning algorithm like KNN, SVM and Decision tree are also analyzed.
**Keywords:**Vehicular communications, V2V, V2I, I2I, Machine learning, Security.

## 1. Introduction

The world is moving towards the artificial intelligence; vehicles are no more exceptions to it. Intelligent transportation systems are one of the examples where the driverless vehicles are increasing in number and withdrawing a strong network of interconnected vehicles if combine with machine learning techniques can yield better results. While moving in network of interconnected ad hoc vehicles security issues will also arises and only cryptographic techniques will not be sufficient to detect and prevents such security violations. Along with traditional cryptographic approaches if newer machine learning technology is added this will definitely add the robustness to security services.

Overall security is important in all aspects of hardware and software technology, vehicular communication is no exception. A small violation in security will lead to large scale hazards might results in road accidents which leads to manual as well as financial loss and inconvenience. There are various security issues which are pointed out by various researcher in their work. Some of the work done by researcher in order to detect and prevent security violations are studied in literature review of this paper. Rest of the paper will first focus on basics of Vehicular communication, security issues involved in it are discussed, Machine learning approaches to solve the security violations are discussed and finally brings Misbehavior detection mechanism framework is shown here.

## 2. Literature Review

centralized mobile wireless networks, ad hoc networks do not depend on any fixed infrastructure. Instead, each node rely on other to keep the network connected. Due to unique properties, ad hoc networks there is a trend to adopt ad hoc networks for commercial use. As wireless network the nodes in Ad hoc network can be movable called it as Mobile Ad hoc network (MANET).

Das and Singh (2020) have elucidated about Vehicular communication for Smart system which is one of the growing research area, Central infrastructure is absent in VANET and use peer to peer networking. VANET as a new wireless technology use wireless access devices to establish connectivity between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). 5 G millimeter waveband is under study to provide ultra-low-latency for vehicular communication. During V2V communication, each vehicle acts as a mobile router and an on-board unit (OBU) is used in each vehicle to communicate with the other vehicles. OBU is responsible for data collection from different sensors and communication with other OBUs. Road side unit (RSU) is in infrastructure which enables communication to the outside network and communication technology—wireless

admittance in vehicular environment (WAVE) supports multi-hop communication between vehicles. The primary objective of VANET was to reduce potential accidents and reduce congestion and delay due to road traffic.

Information safety is considered to be one of the most important issue in VANET, Growing ITS (Intelligent Transport system) leads to various attacks on system, there can be delay to message delivery, Denial of service attack, eavesdropping attack, sending bogus information, spoofing, Sybil attack, privacy attack, data trust attack, replay attack, physical tampering, brute force attack, black hole attack, traffic analysis, illusion attack. The Security of VANET greatly depends on the secure delivery of message. Kaur (2018) has described entities concern with VANET security like vehicles, infrastructure, driver, third parties, attacker and also mention security requirement in VANET. There can be various classes of attack in VANET sorted from layer 1-5.

As Deeksha et al (2017) have mentioned, VANET facilitate vehicles to give information about safety through its communication with other vehicles included in VANET security which can be achieve with various countermeasure. It is found that Encryption and authentication plays an important role in VANET security.

In current safety system the detection algorithm are used to detect attack which cause delay overhead, Rosaline Marry et al (2013) have defined attacked Packet detection algorithm (APDA) which is helpful to detect Denial of Service(DoS) attack and minimize overhead delay and can detect attack in early manner overall improve security.

Authentication is provided to prevent nodes in VANET from various attack and block unauthorized node and this secure data transmission is arrange in cluster in timely manner. Vampire attack attacks on cluster head in cluster where routing depletion affect the path and resource depletion affect the power and bandwidth. To prevent VANET from this attack Jagnade et al (2016) have introduced a technique of Low Energy adaptive Clustering Hierarchy (LEACH) protocol. Hence increases network lifetime and usefulness of system.

Yan et al. (2008) have introduced the concept of security through active position detection. As Vehicle position is one of the most valuable pieces of information in a Vehicular Ad hoc Network (VANET), it can be used to prevent a Sybil attack which is launched by forging multiple identities. These false identities will give the illusion that there are additional vehicles on the roadway, which may have a serious effect on a VANET. For example, a collision warning application given fake vehicle positions may be tricked into thinking that an accident is imminent, prompting the driver to brake quickly, possibly causing a real accident. The solution to prevent most of these attacks is to provide secure topology information in VANETs and to build a secure network for applications, such as a congestion alert system. Underlying solution is the famous adage: ‘‘Seeing is believing” which uses on-board radar as the virtual ‘‘eye” of a vehicle and Global Positioning System (GPS) coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles to achieve local security. By enlisting the help of on-board radar to detect neighboring vehicles and to confirm their announced coordinates, local security is achieved here and Local security is extended to achieve global security by using preset position-based groups to create a communication network and by using a dynamic challenging mechanism to confirm remote position information.

Mejri et al (2014) have mentioned about the communication architecture of VANETs and outlines the privacy and security challenges that need to be overcome to make such networks safety usable in practice. The classification of VANET in VANET from a cryptographic point of view is Attacks on availability, availability, authentication, non-repudiation/accountability, integrity and data trust.

Manivannan et al (2020) have surveyed the secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs) in last 10 years based on tools and technique used in excellent way.

VANET is an emerging technology in wireless communications which has the prospect to improve traffic safety and efficiency, as well as reduce air pollution. The traffic related messages transmitted between vehicles and roadside units must be signed and verified without revealing the real identities of the vehicles. However, an authorized trusted party must be able to obtain the real identity of a vehicle on a controversial message. Some conditional privacy-preserving authentication (CPPA) schemes in VANETs either rely on a tamper-proof device or complex mathematical operations such as bilinear pairing and map-to-point hash function or cannot meet the privacy and security requirements in VANETs.

| Sorted Security Issue | Its detailing | Attacks intricate |
|---|---|---|
| Layer 1 | Network layer attack | • Denial of service Attack<br>• Node Impersonation Attack<br>• Black hole attack<br>• Sybil attack<br>• Masquerading attack<br>• Brute force attack<br>• Distributed Denial of<br>• service Attack<br>• GPS spoofing attack<br>• Worm hole attack |
| Layer 2 | Application Attack | • Bogus information attack<br>• safety application attack<br>• non safety application attack<br>• broadcast tampering attack<br>• Illusion attack<br>• Message alteration attack |
| Layer 3 | Time related attack | • Peer to peer timing attack<br>• Timing attack for authentication<br>• Extended level timing attack |
| Layer 4 | Social Attack | • Social engineering attack |
| Layer 5 | Goggling attack | • Man in the middle attack<br>• Traffic analysis attack |

Table.1 Security Attacks Sorting Into Layers

Samara et al (2010) have also studied various attacks in VANET and studies its solution. An analysis of VANET attack and attackers is shown here. The various security concern like attack and attackers are enlisted along with the security requirement like availability authentication, non-repudiation, real time constraints, confidentiality also overviewed with its probable solution.

**2.1 Security needs of Vehicular communications**

When any vehicle moves in Intelligent vehicular environment there are many safety measures needed. Secure communication among vehicles leads safe road trips. Following parameters of security services available for Vehicular communication

**Availability**: Vehicular communication become unsafe for vehicles when there are more network jams and more message traffic occurs. Sometimes it is genuine and Mant times it is created by malicious nodes intentionally leads to denial of service attacks which ultimately cause hazards to security service known as availability.

**Confidentiality:** Confidentiality requirements means protecting the message so that unauthorized parties cannot disclose it. ITS services are meant for physical safety of passengers on vehicles. Even if a vehicle that is not legitimate is involved in accident, then the legitimate vehicle may be affected. So, the main goal of maintaining confidentiality services is to deliver safety messages to all the users

in VANET. However, for certain applications, the receiving vehicles should process the message only if confidentiality has been guaranteed. Therefore, the messages in VANETs need to be signed and verified using source authentication. Source

**Authentication:** In safety application, the illegitimate vehicles must be prevented from generating safety messages as these vehicles do not have any proof of authenticity. Only those broad casted messages can be considered which are signed by authenticated user. This may be one of the basic requirements for vehicular communication services as these message are broad casted by a number of vehicles. Authentication also helps to distinguish between legitimate and illegitimate vehicle in the VANET.

**Nonrepudiation:** Vehicles injecting malicious message in the network must be identified reliably so that they can be isolated from the network. By incorporating digital signature, the vehicular network can help in providing nonrepudiation property.

**Privacy Protection:** As a wireless technology becomes pervasive where the users are worried about individual's anonymity and non-traceability. However, guaranteeing anonymity and non-traceability may require enforcing non repudiation. The privacy and security must be applied to both safety and non-safety applications. Network operators and governmental authorities use legitimate process for traceability. But, if an attacker knows who is sending message, what one is sending, which application is one using and where he is going etc., then it can have severe consequences and hamper the whole security of the VANET as described by Moustafa and Bourdon (2008). However, non-traceability is one of the most challenging requirements to achieve in VANET as attackers can manipulate the sensitive information.

**2.2 Security Proposals of Vehicular Communications**

Vampire attack attacks on cluster head in cluster where routing depletion affect the path and resource depletion affect the power and bandwidth. To prevent VANET from this attack Jagnade et al (2016) have introduced a technique of Low Energy adaptive Clustering Hierarchy (LEACH) protocol. Hence increases network lifetime and usefulness of system.

Yan et al. (2008) have introduced the concept of security through active position detection. As Vehicle position is one of the most valuable pieces of information in a Vehicular Ad hoc Network (VANET), it can be used to prevent a Sybil attack which is launched by forging multiple identities. These false identities will give the illusion that there are additional vehicles on the roadway, which may have a serious effect on a VANET. For example, a collision warning application given fake vehicle positions may be tricked into thinking that an accident is imminent, prompting the driver to brake quickly, possibly causing a real accident. The solution to prevent most of these attacks is to provide secure topology information in VANETs and to build a secure network for applications, such as a congestion alert system. Underlying solution is the famous adage: ''Seeing is believing" which uses on-board radar as the virtual ''eye" of a vehicle and Global Positioning System (GPS) coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles to achieve local security. By enlisting the help of on-board radar to detect neighboring vehicles and to confirm their announced coordinates, local security is achieved here and Local security is extended to achieve global security by using preset position-based groups to create a communication network and by using a dynamic challenging mechanism to confirm remote position information.

Mejri et al (2014) have mentioned about the communication architecture of VANETs and outlines the privacy and security challenges that need to be overcome to make such networks safety usable in practice. The classification of VANET in VANET from a cryptographic point of view is Attacks on availability, availability, authentication, non-repudiation/accountability, integrity and data trust.

Manivannan et al (2020) have surveyed the secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs) in last 10 years based on tools and technique used in excellent way.

VANET is an emerging technology in wireless communications which has the prospect to improve traffic safety and efficiency, as well as reduce air pollution. The traffic related messages transmitted between vehicles and roadside units must be signed and verified without revealing the real identities of the vehicles. However, an authorized trusted party must be able to obtain the real identity of a vehicle on a controversial message. Some conditional privacy-preserving authentication (CPPA) schemes in VANETs either rely on a tamper-proof device or complex mathematical operations such as bilinear pairing and map-to-point hash function or cannot meet the privacy and security requirements in VANETs.

**2.3 Machine Learning based security**

VANETs based safety models require high reliability and low latency in their performance. Machine Learning/Deep Learning algorithms can be one of the milestone for security issues analysis and detection in VANETs. The success of ML/DL count on the model ability to handle the dynamic nature of vehicular networks. Eziama et al (2018) have developed the trust model which provides a data-driven approach in solving the security challenges in dynamic networks. Here the classification process and the extraction of relevant features using a hybrid model like Bayesian Neural Network is used to create trust model and combines deep learning with probabilistic modeling and effective generalization in trust computation to identify honest and dishonest nodes in the network for smart decision.

Wireless medium allow access to any spreading packets for an intruder in the area, and decentralization in VANET allows any random node to involve in packet forwarding. Because of this the faulty or malicious node can simply affect integrity, availability or confidentiality of the network. There are many more measures taken to prevent or detect misbehaving vehicles/ nodes in the network. The first is known as Intrusion Prevention System (IPS) which are programmed to detect the unauthorized or malicious node to access the data and by this is validate the integrity of the network, the latter is an Intrusion Detection System (IDS).Zeng et al (2018) have introduced the combination of a modified promiscuous mode along with Support Vector Machine (SVM) classification establish a precise trust score table for both IPS and IDS in VANET. Every node/ vehicle in network in packet forwarding route checks the behavior of their next hop to detect if there is any signs of a mischievous node and whether it can affect the performance of the system.

As a mean to improve safety and convenience on the road, Vehicular Ad Hoc Networks (VANETs) provide various advantages to passengers. However, considering that it is a wireless ad hoc type network, it is usual to see numerous security exploits present in the environment. There are prevention methods as well as responsive solutions for network intrusions; the former is known as Intrusion Detection System (IDS), which monitors and detects potential intrusions that are ongoing in the network. Active network attacks are generally designed to reduce or interrupt availability of the network. Effect of these attackers on the network can be measured by select parameters, which can in turn be used as the main lead for detecting malicious behaviorsShamsa et al (2018) have elucidated IDS in VANET using the combination of modified promiscuous mode for data collection and Support Vector Machine (SVM) for data analysis to establish a shared trust value for every vehicle on the network as Trust Aware SVM Based IDS (TSIDS).

Zeng et al (2018) have enlightened an intrusion detection system that deals with monitoring malicious activity. VANET have IDS but machine learning based intrusion detection system is robust in environment changes which is frequent in VANET.

Intruders can be passive or active violating the privacy of users or disrupting and otherwise consistent data flow. Trust Aware SVM-Based IDS use modified promiscuous mode in an efficient way together with SVM for analyzing active network nodes and mark them as trusty or malicious vehicles based on the reputation of their performance data gathering, we use promiscuous mode with

altered behavior for more efficiency and security to capture and analyze packet headers. As SVM is a reliable machine learning tool for various non-linear classification scenarios

Intrusion detection systems plays a vital role in detecting malicious activities that integrate the performance of the vehicular network. The distributed nature and the limited resources available, present a considerable challenge for providing security to these networks. The need for an intrusion detection system (IDS) that can acclimate with such challenges is of extreme significance. The IDS mentioned in Amouri et al (2020) composed of two stages; stage one collects data through dedicated sniffers (DSs) and generates the CCI which is sent in a periodic fashion to the super node (SN), and in stage two the SN performs the linear regression process for the collected CCIs from different DSs in order to differentiate the benign from the malicious nodes. The detection characterization is presented for different extreme scenarios in the network, pertaining to the power level and node velocity for two different mobility models: Random way point (RWP), and Gauss Markov (GM). Malicious activity used in the work are the black hole and the distributed denial of service (DDoS) attacks.

As VANET's wireless communication increase driver's and vehicle sensors line-of sight, hence enhancing situational awareness. The safety and performance of VANET depends on exactness of data exchange, location spoofing can be one of the menace for it. Steven et al (2018) have explored the common ML techniques and provide detection scheme baseline to the machine learning community. Plausibility check is used to validate correctness of data. Here Location Plausibility Check and Movement Plausibility Check are integrated into feature vector then supervised ML techniques like K-Nearest Neighbor and Support Vector Machines (SVM) are implemented to improve the overall Precision value of misbehavior detection system. He proved that a misbehavior detection system that uses plausibility checks and machine learning provides 20% higher accuracy and maintains a recall within 5% percent of the recall of plausibility checks.

**2.4 Tabular Literature review**

| Sr. No. | Year | Author | Techniques and Description | Accuracy and Observations/Remarks |
|---|---|---|---|---|
| 1 | 2020 | Debasis Das, Arun Singh | Vehicle to Vehicles (V2V), Vehicle to Infrastructure (V2I), OBU, RSU. | Detailed technical aspect of VANET and its features are discussed. |
| 2 | 2018 | Rajdeep Kaur | VANET security attacks | Various VANET attacks like Network attack, application attack are summarized. |
| 3 | 2013 | M.RosalineMarry, M.Maheshwari, M.Thamaraiselvan | Attacked Packet detection algorithm (APDA), DDoS attack. | APDA is helpful to detect Denial of Service (DoS) attack and minimize overhead delay in early manner. |
| 4 | 2016 | Gayatri Jagnade, Saleha Saudagar, Sonika Chorey | Low Energy Adaptive Clustering Hierarchy algorithm called as LEACH in short and a vampire attack | LEACH protocol is used to secure VANET from vampire attack |
| 5 | 2020 | Gaurav meena, Deepanjalisharma | Use Machine Learning, Genetic Algorithms, Soft Computing, Image Processing | Can predict accurate and timely traffic flow Information |
| 6 | 2018 | Eziama et al. | Bayesian Neural Network(BNN), Deep leaning, probabilistic modeling for intelligent decision | Relevant features are extracted for malicious node detection using DL and develop trust model. |
| 7 | 2018 | Zeng et al. | Intrusion Detection System, Vehicular Technology. | Describe about an intrusion detection system that deals with monitoring malicious activity |
| 8 | 2018 | Erfan et al. | Intrusion Detection mechanism(IDM) and Support Vector machine (SVM) | Detection of any type of intrusion using supervised SVM machine learning method |
| 9 | 2018 | Steven et al. | IDS, SVM, K-Nearest Neighbors (K-NN). | Perform malicious node detection using KNN and SVM |
| 10 | 2017 | Fuad et al. | Artificial Neural Network (ANN), traffic dataset called NGSIM(Next Generation Simulation) | It worked on Misbehavior Detection Model using ANN for VANET |

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

### 3. Proposed architecutre Vehicular communications

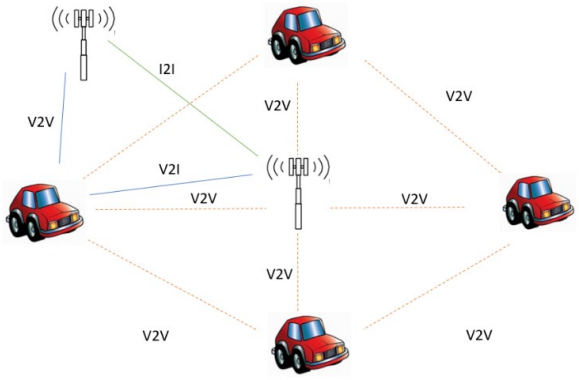


Figure 1. Vehicular Communication Architecture

Diagram shows Vehicular communications where vehicle to Vehicle(V2V), Vehicle to Infrastrucure(V2I) and Infrastructure to Infrastructure(I2I) proposed architecture which runs on IEEE802.11p Wireless LAN and peer to peer networking. It is decentralized architecture where vehicles also acts as a medium for transmission.

**Conclusion**

Overall security is important in all aspects of hardware and software technology, vehicular communication is no exception. A small violation in security will lead to large scale hazards might results in road accidents which leads to manual as well as financial loss and inconvenience. Thus concluded, Machine learning approaches used along with cryptographic methods can result in one of the robust attack detection scenarios.

**References**

[1] Das D., Singh A., 2020, “Vehicular Ad hoc networks”, science and education magazine Techspace: IIT Jodhpur.
[2] Kaur R., 2018, “Security Issues in Vehicular Ad-hoc Network (VANET)”, Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI).
[3] Samara G., Al-Salihy W. A. H., Sures R., 2010, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)", *Second International Conference on Network Applications, Protocols and Services*, Kedah, 2010, pp. 55-60.
[4] Moustafa, Hassnaa, and Gilles Bourdon. "Vehicular networks deployment view: Applications, deployment architectures and security means." *Ubiquitous Computing and Communication Journal, special issue on Ubiquitous Roads* 3 (2008).
[5] Jagnade G., Saudagar S., Chorey S., 2016, “Secure VANET from Vampire attack using LEACH protocol”, *SCOPES IEEE Xplore.*
[6] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." *Vehicular Communications* 1.2 (2014): 53-66.
[7] Manivannan D., Moni S. S., Zeadally S., 2020, “Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs)”, Vehicular Communications, Volume 25, 100247, ISSN 2214-2096.
[8] Eziama E., Tepe K., Ali Balador, Nwizege K. S., Luz Jaimes M. S., 2018, “Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning”, *IEEE global com workshop.*

[9] Shamsa E.A., Rizanerb A., Ulusoyb A. H., 2018, "Trust Aware Support Vector Machine Intrusion Detection and Prevention System in Vehicular Ad hoc Networks", *published in Computers and security.*

[10] Zeng Y., Qiu M., Ming Z., Liu M., 2018, "A machine leaning based intrusion detection in VANET", *International conference on Smart computing Communication.*

[11] Amouri, Amar, Vishwa T. Alaparthy, and Salvatore D. Morgera. "A machine learning based intrusion detection system for mobile Internet of Things." *Sensors* 20.2 (2020): 461.

[12] So Steven, Prinkle Sharma, and Jonathan Petit. "Integrating plausibility checks and machine learning for misbehavior detection in VANET." *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2018.

[13] Saudagar, S.I., Chorey, S.A., Jagnade, G.A. Review on Intrigue Used for Caching of Information in View of Information Density in Wireless Ad Hoc Network. In: Advances in Intelligent Systems and Computing, vol 814. Springer, Singapore(2019).

[14] Saleha Saudagar,Dr. Rajendra Prasad Mahajan," Solving Vehicular ad hoc network issue using machine learning", International journal of creative research and technology, Vol 9 Issue 4, April 2020.