Intelligent and Secure Vehicular Network using Machine Learning

Manmohan Sharma and Heena Khanna

School of Computer Science and Engineering,
Lovely Professional University, Phagwara, Punjab, INDIA.

Abstract

Vehicle to vehicle communication is a crucial aspect in transportation at this age and the major concern is to have a secure network of communication for not only vehicle to vehicle but also for vehicle to infrastructure which includes the communication with RSU (Road Side Units). The main aim behind efficient vehicular communication is the safety of the driver and better traffic management with a target to have zero fatality transportation system. Jitter, PDR, TDR and throughput are the major factors to deal with while designing the algorithm. Machine Learning has been instrumental in providing solutions to the Secure V2V and V2I communication. This article talks about the basic concepts, challenges and the recent work done by researchers in the field. Towards the end Open Issues are addressed with the future scope of work.

Keywords: V2V, V2I, Machine Learning, DoS Attacks, QoS, Guaranteed Throughput

1. Introduction

1.1 Vehicular Communication System

The Communication between two or more vehicles while running on the roads is said to be V2V Communication coined by Wu, et al. [15,31]. The vehicles share the information about their speed, sudden turn, location, direction, brakes and also for SOS, this helps the vehicle to avoid any potential crash. Vehicles hereby communicate over Mesh Network to receive, send and further retransmit signals. Its range is up to 300 meters as observed by Yong Hao [33] and it sends messages in omni-direction creating 30 degrees awareness in the vicinity (US Department of Transportation). The communication is established by Dedicated Short Range Communication (DSRC). DSRC is a dedicated wireless communication channel used to establish one way or more short-range connections for automotive usage. DSRC is a standard which is approved by Federal Communication Commission (FCC) and International Organization Standard (ISO).

Another variation to it is where Vehicle talks to any other physical device and is termed as Vehicle to Infrastructure. Tahir et al. [30] also termed it as Internet of Vehicles on the lines of Internet of Things (IoT).

If used effectively, V2V can increase the safety on roads and can help decrease the number of fatalities on road to an extensive rate. And it can even help a driver to send SOS message to nearby Vehicles in case of any medical emergency. A major obstacle to achieve a complete automotive system which is V2V enabled is the agreement of all automotive manufacturers to include the required hardware in all of their products.

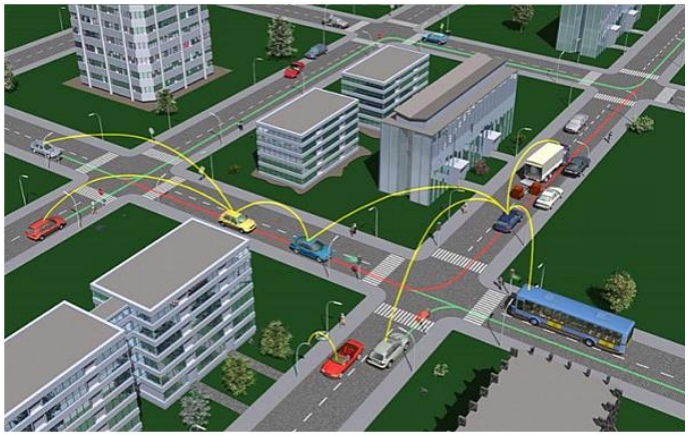

Figure 1 V2V

(Source: ITS- US Department of Transportation)

1.2 C-ITS

Cooperative Intelligent Transport Systems are vehicles related communication protocols which are speedily being developed at International Level. It not only encompasses the communication amongst road vehicles but also other means of transportation too including air, water and railways which can further be connected with back offices as well. C-ITS comprises of various communication levels as in Vehicle to Infrastructure, V2V, Vehicle to Individual etc. proposed by Zhu, et al. [34].

Many countries have already approved new rules to accelerate the deployment of C-ITS enables transport system. EU has recently approved the norms for near zero road fatality and injury program wherein they plan to achieve it under their Vision 2050 initiative. Here they are aiming at sharing only the important information required for the smooth travel of the vehicles and nothing which includes driver's and vehicle's credentials. All the data will be share in compliance to European Data Protection described by Tahir, et al. [30].

1.3 Road Fatalities

It is heartening to mention that India has the highest number of Road Fatalities in the world. As per the reports of 2016, more than one third road accidents deaths were marked for India. As per WHO Global Status Report on Road Safety 2018, the count of deaths on roads is increasing tremendously and touched 1.35 Million in 2016. Whereas the number of injured crossed 50 million. Some projections claim that by 2020, Road accident will be third biggest cause of death. Apart from poor road condition and poor safety norms, one major reason is sudden collision of vehicles. It is the time when better system incorporating the technology with automobile to bring a halt to this unwanted threat to our lives discussed by Yadav et al. [32].

1.4 Types of Attacks

There are various threats involved in data transfer which is affecting V2V communication adversely. The primary one which is considered is DoS attack which is segregated in Application and Network modes by Parmar [7].

Application mode covers all those attacks which send incorrect message to the driver and also diverts them to some incorrect path. This includes Sybil Attack and Message Suspension Attack. **Sybil Attack** is an attack where in the attackers creates an illusion of a large number of vehicle set and then sends the message to the target vehicle to misguide the vehicle/driver discussed by Grover [10]. On the other hand, **Message**

Suspension Attack is the one where the attacker suppresses a message and sends it later to the victim on some other time for its own personal benefit.

Network Mode comprises of all those attacks wherein the bandwidth is blocked and delusion of jammed network is given. Fabrication under network mode is a kind of attack where the real message is fabricated. **Alteration Attack** is the one where the real message is altered and the altered one is sent to the victim. **Replay Attack** is also a kind wherein an old message is sent again and again, it confused the authority and also to prevent the identification during accident cases.

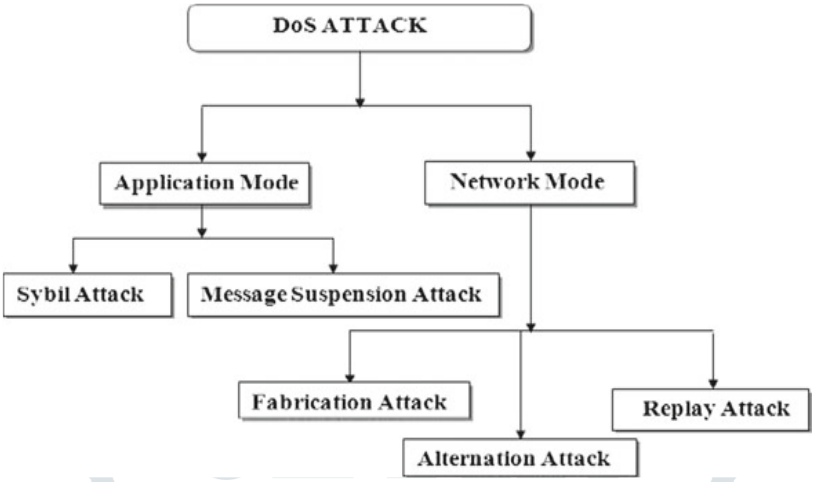

Figure-2: Dos Attack

(Source: Karan Verma [12])

1.5 Machine Learning

It is an Application of Artificial Intelligence wherein a software or system learns on its own with the experience and behaves according to the past patterns without being programmed by Humans every time. Machine Learning is a process of creating systems that can access the data and use them for decision making. Some of the day to day applications of Machine Learning are Virtual Personal Assistant Siri, Alexa etc. Machine Learning has brought a revolution in Computer Science World by engaging large data sets to be evolved in a self-learning process and produce results like never before which further keep improving. ML can be further divided into three major categories described by Liang, Ye, & Li, [13]

1.5.1 Supervised Learning

It is a mechanism where we have a labelled training set with each sample labelled with a class. This labelled data is used to formulate an algorithm to find out the results. It is further divided into Classification and Regression. Classification comprises of the algorithm which work for categorical data and regression works for numeric data and both gives us the prediction on the basis of the algorithm generated by the labelled data.

1.5.2 Unsupervised Learning

It is the second most popular category of Machine Learning algorithm which works on Unlabelled Data. The real time data can't always come with label and therefore the need for a mechanism which can work on unlabelled data and hence Unsupervised Learning was introduced.

- **Clustering** is the most commonly representative for Unsupervised Learning, in which the data with similar behaviour is grouped together in one cluster and so on. There are many Clustering algorithms like K-Means, K-Medoids, Hierarchical Clustering and few others.
- Another Unsupervised Learning case is **Dimension Reduction**, in this high dimensionality data is reduced to lower dimensions for better results and inference.

1.5.3 Reinforced Learning

It is an interesting field for ML. Here the agent learns on its own without observing someone else's behaviour. The whole learning process is dependent upon the reward process. The agent is rewarded every time the agent performs well and on the basis of the reward system the action is improved. Reinforcement learning can be applied to provide a secure and hassle free V2V Communication.

2. Related Work

Feng & Haykin, [6,8] proposed a method to detect real time detection of radio jamming Denial of Service attack via IEEE 802.11p in Vehicle to vehicle(V2V) communication. The main aim is to find out the reasons of periodic loss of cooperative awareness messages (CAM) in a platoon of vehicles. The method proposed by them allows the operation in real time jitter with every CAM transmission. Two jamming models are considered in this paper: ON-OFF and random.

Patounas, et al. [24] worked on evaluating the wireless communication between vehicles along with the physical working of Vehicles on a Platoon. They did a complete study of VANET and ITS, also emphasized on their role in future transportation. Here they implemented and tested defence methods against jamming. Primarily three methods are discussed, data redundancy, inference reduction, warning systems for on board vehicles. The results shown are positive and help increase the resilience to attacks while vehicle Platooning.

Lyamin, et al. [17] discussed at length about the existing studies on Jamming Models over VANET and comparing the existing detection methods. Further they used AI to address the real time problem of detecting Jamming over V2X. They proposed hybrid jamming detector with data mining capabilities infused in statistical network traffic analysis which gave an acceptable performance despite of random jitters during the generation of CAMs.

Lyamin, et al. [18] focused on jamming under periodic positioning messages called beacons exchanged by the platoon vehicles. Probability for both false alarm and attack detection is estimated and finally a method is proposed for real time detection of Denial of Service attack in IEEE 802.11p Vehicular Ad Hoc Network (VANET)

Bilal [3], Lyamin, et al. [16] and Noori [22] conducted a number of simulation experiments to check the efficiency of ITS Vehicular Communication over platoon. They further assessed fuel consumption of platooning. Their study showed that communication setup influences the platooning fuel efficiency.

Lyamin, et al. [19] evaluated the performance of DCC for cooperative driving applications while identifying the ways to improve. They further derived that there is a negative impact on the performance of cooperative vehicle applications when proper DCC parameterization is not done. A detailed study is also done describing how DCC is a mandatory component of the 5.9 GHz ITS-G5 vehicular communication protocol working with range degradation, self-interference and channel load.

Llatser, et al. [14] worked broadly on a new paradigm i.e. frequency of messages. They defined a performance metrics which calculate reliability, latency and data age of communications sent over vehicle convoy in Inter Vehicle Communication (IVC). They derived that there is a direct relation between the communication performance and the frequency of convoy messages which means when the message frequency is high, the number of lost messages is increased whereas a low message frequency ensures higher data age. Therefore, they suggest the algorithm designers to optimally choose the frequency of messages.

Badea [2] has done a brief and state of the art survey to describe all the latest trends in IoT networks in Vehicular Communication field. They also introduced GEX2017/MTSR research project and their proposed solutions in the same field. Issues like security and vehicular fleet management were also discussed t length.

Abdulhakim [20] presented a distributed MAC (Medium Access Control) design PECA (Performance Enriching Channel Allocation) for channel allocation in a shared network. This model reduces the collision caused by CSMA/CA as MAC. It experimentally proved that PECA model reduces the collision, and maximizes the throughput. It also ensured successful packet transmission under a highly congested VANEt

all the experiments are conducted in different environments such as City, Highway and Rural (CHR). Kamini [11] discussed the parameters and application of VANET.

Elleithy [5] proposed **"**Secure Intelligent Vehicular Network using fog computing" (SIVNFC) wherein they have integrated Fog Computing with Hybrid Optimization Algorithms such as Firefly Algorithm, Cuckoo Algorithm, firefly neural network with Key Distribution Establishment (KDE). This model first classifies between the genuine and attacking vehicles through firefly neural network with is a feedforward back propagation network then the network and node level attacks are checked for authentication using above algorithms. SIVNFC is also compared with other algorithms to check the Quality of Service parameters – Jitter and Throughput.

Hasrouny et al. [9] proposed a trust-based communication system using on PKI (Public Key Infrastructure). Herein they present a group-based trust management and revocation system. In this algorithm any detection of misbehaviour will trigger a hierarchical revocation for unwanted vehicle/entity. It is very light weight solution for trust evaluation and revocation. The security issues of networks and its solution discussed by Oğuz [23].

Muraleedharan and Osadciw [21] addressed the issues like response time, aging of data, packet delivery, bandwidth, message prioritization and communication cost. To deal with these concerns they used cognitive security protocol, this protocol disseminates the packets using distributed sensor technology and at the same time prevents data aging and efficient QoS with fighting against DoS attack. The protocol proposed here focuses primarily on response time and message authentication, confidentiality and non-repudiation.

Sharma [28] applied AI to achieve a secure wireless communication over VANET. Spoof messages and falsification of meter reading have been mentioned as major security threats. Message authentication and DoS attack are balanced out by searching the pivot point. Context-Adaptive Signature Verification strategy is used to authenticate the messages and AI is used to reduce communication and computation overhead. This study used a traffic road simulator SUMO, data network simulator OMNET ++ and Veins a VANET Simulator to analyse various real time attacking scenarios. The output of the experiment presents a effective design choice for securing wireless communication over VANET.

Ye and Li [13] discussed about the major issues in V2V communication due to large volume of data and suggests Machine Learning as solution to the same. To optimize the network performance machine learning techniques are suggested at length.

Silas [29] have proposed and logarithm named PSO (Particle Swarm Optimization) to detect and prevent DOS in VANETs. This paper discusses many other algorithms for prevention and detection of DOS and a comparatively better solution is proposed.

Feng and Haykin [6] proposed a solution inspired by predictive adaption feature of Human Mind based on task switching. They propose a tool called Cognitive Dynamic System and uses its function Cognitive Risk Control to ensure the output. It selects the channel on the basis of risk level evaluation. Simulation is used to prove that this solution is able to defend hybrid attackers under different settings.

Rowan [27] Signal and sensing devices are discussed for the usage in communication. An inter vehicle session key generation is proposed which further is aligned with block chain public key. This solution helps primarily for saving the time used in handshake.

Elleithy [5] Vehicular Cloud and Fog Computing combined with hybrid optimization algorithm including some algorithms for Swarm Intelligence namely Cuckoo and Firefly algorithm to detect real time detection of DoS attacks in IEEE802.11p. Here they have used Firefly Feed forward back propagation neural network (FFBPNN) as a classifier to segregate between genuine and affected vehicles. The proposed scheme is compared with Cuckoo/CSA ABC and Firefly GA by considering jitter, throughput, and prediction accuracy.

Sahil Garg [25] developed a smart security framework for VANETs equipped with edge computing nodes and 5G technology has been designed to enhance the capabilities of communication and computation in the modern smart city environment. It has been experimentally demonstrated that use of edge nodes as an intermediate interface between vehicle and cloud reduces access latency and avoids congestion in the

backbone network, which allows quick decisions to be made based on the traffic scenario in the geographical location of the vehicles. The proposed scheme outperforms the conventional vehicular models by providing an energy-efficient secure system with minimum delay.

Alomari et al. [1] proposed two novel dynamic movement techniques that offer obstacle-avoidance path planning for mobility-assisted localization in WSNs. The movement planning is designed in a real-time using two swarm intelligence based algorithms, namely grey wolf optimizer and whale optimization algorithm. Both of the proposed models, grey wolf optimizer-based path planning and whale optimization algorithm-based path planning, provide superior outcomes in comparison to other existing works in several metrics including both localization ratio and localization error rate.

3. Discussion

Vehicle to Vehicle(V2V) communication is one of the recent fields of research who has gained attention from all over the world whether it is the research industry or the commercial industry. V2V communication may involve two or more Vehicles interacting with each other to exchange the data. Automation of any field leads to reduce the human effort and to production of efficient result. There are several issues which the automation in the field of V2V communication. The V2V communication can be viewed in a network "Net" with "n" number of nodes following a communication protocol P. As mobility is an integrated part of the V2V communication, security concerns like threat prevention, handling of data volume above a given threshold becomes a common practice for such kind of network. A network becomes more prone to security threats when the mobility becomes an essential part of the network. The network administrator will have to put a lot of manual effort in order to understand what exactly is right and what exactly is wrong. Some of the previous research architectures have tried their hands in solving the security measures by applying the rule set architecture which is successful for small set of networks. As the scalability comes into play, it becomes hard to manage thousands of rulesets at one time. Instead of scanning thousands of rulesets at once consumes a lot of time which delays the network. Delay means the unnecessary time which is spent in order to transfer the data. It can be also termed as the difference of the actual time consumed in the network and the expected time consumed in the network in order to transfer the data packets. Distributed Denial of Service (DDoS) attack is a commonly observed security threat in V2V communication network in which the server faces a lot of service requests which often goes out of the boundary limit of the serving capacity and that leads to either deadlock or packet dumps which eventually reduces the Packet Delivery Ratio (PDR).

$$PDR = \frac{Received_{Packet}}{Sent_{Packets}} \quad (1)$$

There are other similar intrusion structures which are either advancements of DDoS or follows similar architecture as that of the DDoS attack. As for example, Replay-attack sends the same packet again and again to keep the server busy in order to manage the packet identities.

Analysing the existing work in the area following areas are identified to be worked upon.

- Security Monitoring is one of the key aspects of V2V network. Presented algorithm till now has failed to give a complete assurance when it comes to any change of behaviour of any Intruder.
- Lack of the implementation of the adaptive framework is observed when it comes to security protocols. There is no such architecture which is able to prevent multiple threats with single prevention frame.
- Most of the researches have only proposed distance aware communication without analysing the demand and supply frame.
- The current researches used only Lagrange's Interpolation method to find un-trusted nodes, other methods such Spline and the Polynomial Fit can also be considered for better results Erskine [26].
- Most of frameworks are working on DoS or HDSA (Hybrid Dos Attacks) a mechanism can be defined by Elleithy [4] and Erskine [26] to work on multiple threats at the same time apart from DoS related attacks.