IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ANOMALY DETECTION IN AUTONOMOUS VEHICLE USING ML APPROACH

Atul B.Kathole
Research Scholar
Department of Computer Engg.,

Dr.Dinesh N.Chaudhari
Professor
Department of Computer Sci & Engineering
J.D.I.E.T, Yavatmal, India

Abstract

The adaption of the Internet of Things has enabled people to bridge actual objects to the Internet and make people's lifestyles easier. Hackers are familiar with these real-world devices, which make users nervous rather than easy to live. Smart cars are one of the techniques that facilitate our lifestyles, but when an assailant utilizes its flaws, the drivers, as well as the public surrounding us, can suffer seriously. There have been incidents in past years that attackers have targeted Autonomous Vehicles (AVs) that have provided the car full power or network jamming, resulting in loss of knowledge. In this article, we introduce the analysis of a DDoS assault on a network of intelligent autonomous cars in a simulated world. By using our proposed system able to detect the attack in the network to prevent the network issue.

Keywords: Autonomous Vehicles, Cybersecurity, DDoS, Attack Simulation.

I. INTRODUCTION

Most cars of this age have the potential to be intelligent like intercom with other vehicles, infrastructure connectivity, GPS, sensor-driven decision-making, and so on [1]. The independent vehicle is driver-free and can decide on its own based on multiple sources of data (with next to no human input) and escape dangers that do not occur in the immediate vicinity by the occupants or other cars. These vehicles collect data for the driving model that allows crucial motor choices from countless detectors, the Internet, road networks, GPS, and others. Communication is an integral part here, as smart cars provide major information from other smart companies such as smart cars and roadside networks. The VANET(Vehicle Adhoc NETworks) that provides V2V (Vehicles-2-Vehicles) and V2I (Vehicles-2 infrastructure) for communication are used to communicate with other smart organizations. Protocols are based on the DSRC(Dedicated Short-Range Communications System) [3] which provides small-range communication at faster speeds through the WAVE(Wireless Access in Vehicular networks). Due to the high-speed mobility of cars, the importance of this capacity is enormous. The high-speed connectivity assists in reducing slow down that can result in serious effects. VANET has been developed to ensure fast, convenient, and safe passengers ride.

In AV the systems can be widely divided into two parts: protection and non-safety [7].

Safety applications shall provide rider protection information on lane voyages, such as car crashes, whereas systems with non-safety ought to include data such as forward-looking traffic, weather, parking assistance, etc. In addition to being correct and precise, safety information must also be communicated to the passenger in a timely and secure manner, as it is crucial for the human life of the passenger[4]. Network connectivity is thus necessary and it can be deleterious except with a slight delay. In general, hackers initiate a DDoS attack with spamming or resource overriding on the AV [2]. Due to an intruder or multiple distributed attackers, such unavailability will lead to a DDoS attack on the network [9].

As cars get smarter, scientists need to prevent cyber attacks. In the experiment conducted, the network is jammed, and receiving nodes lose messages from the benign host as the period reduces and the number of jammers increases.

DDoS, Eavesdropping, Man-in-the-center are a part of the major frequent forms of cyber threats. As in our work, we will be focusing on a DDoS assault to jam the autonomous AV contact channel [11].

Attacking DoS/DDoS: A variety of communication devices designed to acquire and exchange information required for secure navigation and conduct would be equipped for autonomous cars [11]. These systems can provide vehicle-to-satellite and vehicle-to-vehicle, vehicle-to-internet, and other communications. Contact also takes place via the 'controller area network' within the car itself. Disruption of any of these communication methods can degrade the car's ability to function properly [12].

In our work, we are going to maintain a table that is going to stores the position of each & every node so that we have an entry of each node registered with us to reduce unauthorized access to secure the system from malicious activity.

The DDoS (Distributed Denial of Service) Simulation will be used in this post. The history study on AVs is addressed in section I.A. The related work done on cyberattacks on intelligent cars in Section II is defined. Section III provides a summary of the study deficit, and Section IV describes the proposed experimentation. The end of section V and some of the forthcoming work in this area are discussed.

II. RELATED WORK

With the introduction of technology, its advantages and new problems are for the consumer. Innovations have been studied until they were an unavoidable portion of our lifestyle [12]. Intelligent cars aren't any exception, with 78 percent having problems with intelligent cars before 2016 in their daily life. However, when people see their friends and families using it, this statistic declines dramatically. During the construction of a smart car that depends on knowledge exchanged by other cars, multiple considerations need to be addressed. The latest hacking done by ethical hackers at Jeep Cherokee on a highway in 2015, caused more confusion for the people when all major automakers started improving their algorithms.

There are also unanswered questions, such as what about when the intelligent car does not respond although not compromised, or a certain assailant spreads the wrong data, which can lead to devastating accidents. Although it was an experiment, it opened up the user's room for skepticism. The other factor which was brought on by technology as cyber threats were carried out was which party is liable [13]. A variety of regulatory actors such as conventional OEM suppliers, mobility providers, public authorities, manufacturing bodies, or customers themselves are concerned. The journal article by a leading advisory company, KPMG, provides some suggestions about how the threat is mitigated.

These are the factors mentioned in their report:

1. Organization leadership, and governance.
2. Risk management and compliance.
3. Secure product development.
4. Threat management and incident response.
5. Cybersecurity training and education
6. Industry collaboration and sharing

The standards explain automation levels. The criteria are established. The level of automation is between 0 and 5.Level 0 includes all cars that were entirely manufactured by Porsche from 1967 to the most recent car developed in 2018. Level 1 autonomy allows the vehicle to choose between steering, braking, or acceleration in a restricted area, the advanced driver assistance system (ADAS) mounted inside the car. Level 2 automation involves both steering and acceleration management. ADAS control. The human driver must, however, still be very patient. Level 2 examples include Audi Traffic Jam Support, Cadillac Super Cruise, Tesla Autopilot, and many more. Both facets of a driving vehicle are carried out by level 3 automatically, but once ADAS asks, the human driver is responsible for the checks. The human driver must also be careful. In 'Audi Traffic Jam Pilot' the level 3 automation is available. The next automation stage helps cars to execute all functions and track the environment; no care is expected by the human driver [11]. While ADAS will carry out all the work in the last stage of automation, human beings are just passengers. At level 5, the user has to feed the address to GPS, and without requiring additional assistance or information from the user, the car is immediately taken to its destination. Automotive businesses have so far sought to reach level 3. Tesla says it is level 3 but the Tesla reviews are automated level 2. Illustration 1. The cyber-attack Smart Car Gateways shows some potential access points to cyberattacks on an intelligent automobile [8]. The machine becomes more vulnerable to exploitation by the attackers as the level of automation is increasing.

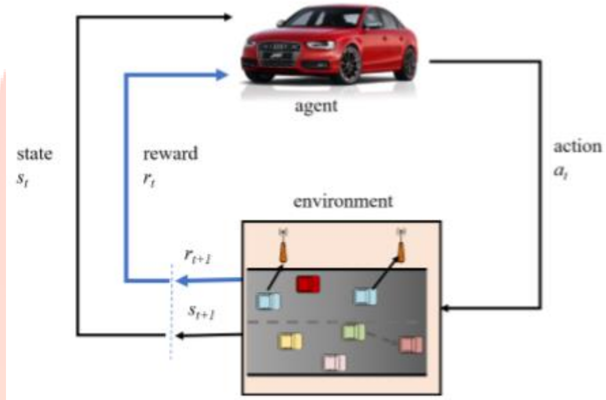

Figure 1. Smart car gateways for cyberattacks

Intelligent cars can communicate across the network, making them susceptible to cyber-attack. The assault will occur if the car is stagnant or moves to its destination. The car itself brings the owner down to an empty street and stops and is better than taking a person home from work. The car itself takes a desert street. An assault may be fatal while the car is moving. In general, cyberattacks are categorized into two groups. First, the software attack which enables the program to read or change its actual sensors is done using hardware with the Electronics Control Unit (ECU) [9]. The second type of classification takes place on software. An early autonomous Uber vehicle failed in May 2018 and resulted in a deadly accident in Arizona. An elderly lady was killed when a pedestrian crossed the lane, which Uber was unable to distinguish. After the incident, internet sources indicated that the program had failed [10][12], while others reported a malfunction in the hardware [13][14][15]. [14]. In all cases, the underlying principle that should be taken into account can be altered, modified, postponed, or jammed in response by beginning a cyberattack, both hardware, and software. DDoS is a cyber threat that could be launched if the hacker accesses either of the ECUs of an intelligent vehicle [12]. The availability of critical components onboard affects. Ideally, the VANET should have a built-in cyber-attack mitigation mechanism, but before then no one claimed to have an intrusion-resistant fully designed detection device. Experiments in the past have been conducted using a Simulator to build an intrusion detection system for the DDoS attack but when nodes of the rogue (attacker) have sufficiently increased [4], the device crashed.

Stefan Mihai et al. [2], explains technical advances leading to a wired, mobile, cooperative transport system. They discuss the most important safety consequences of VANETs which provide a thorough analysis of existing possible methods for keeping vehicle network communications private, stable, which is confidential. However, mass acceptance depends on closing the gap in terms of both secure automobile accessibility and road networks for the remaining open problems. The author also explains the need for coherent methods and governance to ensure flexibility and reliability while upholding appropriate levels of security and privacy. Network security also needs to be strengthened to ensure the safe delivery of the information.

Fabio Gonc lves et al. [3], This paper includes a detailed SLR on the usage of VANET Smart IDs. Ns-2 with SUMO is the most common network-traffic-simulator combination employed in the studies. As for the most common ML algorithm, it appears that NN (its various variants) is the one chosen. For each analysis, the required datasets are usually generated, either from the simulation or the trace file of the network simulator. One of the SLR's purposes was to identify highly credible and publicly accessible datasets. Unfortunately, this does not appear to have been possible. Study assessment shows that most of them don't specifically define how their databases and attacks are being developed. Furthermore, neither of them is making their databases freely accessible for peer analysis. Any of them use freely accessible, commonly reputed databases, such as the Kyoto dataset and the NSL-KDD. They also describe the is engineering as an infrastructure for intelligent identification of attacks. One purpose of this work should be to create large enough datasets to allow the successful training of ML algorithms. Also, a thorough description should be made of how the dataset, attacks, and daily messages were created. Furthermore, this must be made openly accessible for peer review.

The author explaining machine learning (ML), Mohammad Asif Hossain et al. [4], which is one of the fastest developing computational methods, is widely used to resolve critical problems in many fields. Ad hoc vehicle network also referred to as VANET is projected to play a critical role in lowering congestion and road traffic accidents. To guarantee this place an enormous data volume should be exchanged. Present connectivity assigned to VANET is therefore insufficient to accommodate such large volumes of data. Hence VANET goes through a problem of scarcity in the spectrum. Cognitive radio i.e. CR is a potential answer for solving issues of this type. VANET based on CR or CR-VANET could attain many steps for performance improvement including connectivity with low latency and ultra-reliability. ML approaches can also be combined with CR-VANET to make CR-VANET very intelligent, to attain accelerated adaptability to environmental conditions, and to increase service efficiency in an energy-efficient manner. They provide a summary of CR, VANET, CR-VANET, and ML including their architecture, features, problems, and issues that are open. The specification and roles of methods of ML methods were evaluated in scenarios of CR-VANET. It also offers information on the use of ML in automated or driverless vehicles. They also define the implementations and latest advances of methods in ML discussed in different areas of CRVANETs, such as routing, spectrum sensing, security, and resource utilization. ML's functions have been extended to mitigate traffic congestion and road collisions, and many aspects of ML usage of AVs have been identified. Using tools of ML to leverage the rewards of being researched because those fields are only in the early stages. He discussed some of these scopes in his thesis, unresolved questions, and future trends in the field.

WANG TONG et al. [5], In this article, the author deals not only with the design, components, and operations of SDN-based VANETs but also with how SDN-based VANETs allow better communication than traditional VANETs. By handling the network as a whole from a single remote controller it allows us to reduce the total network load. In addition, SDN controllers can track security threats. In this article, they emphasized that this modern vehicle technology aids a great deal in tracking and managing the whole transportation networks that had been problematic before.

At first, the handheld module with versatility and wireless card to connect without a physical medium was developed in our proposed scheme. We also developed and deployed several more mobile vehicles using the proposed terminology, each of which

III. Proposed Work:

In refers to the previously developed module. The mobility speed, direction, and duration of message and interval of each vehicle by which the modules are communicating. At first, we found that there was almost no error and delay in the packet when the simulation was initialized. They also had a few significant network improvements, including adjustments in message length, period, and several nodes [12].

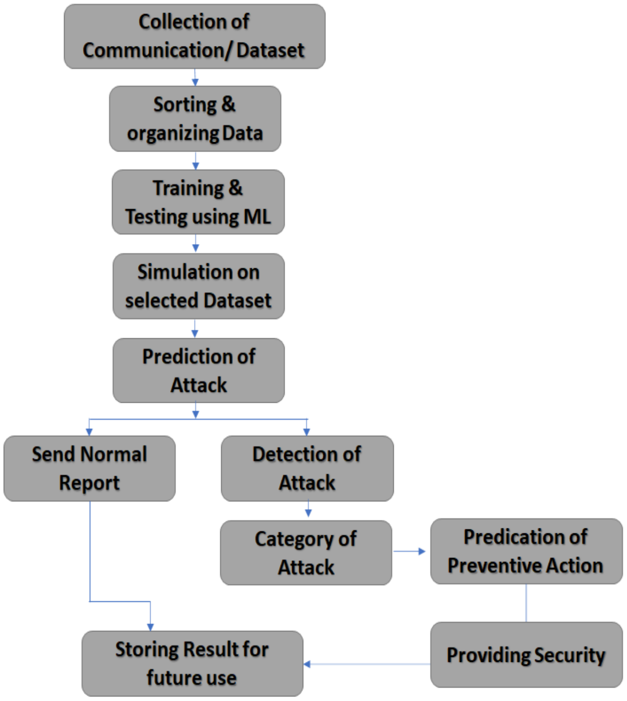
Collection of Communication/ Dataset
Sorting & organizing Data
Training & Testing using ML
Simulation on selected Dataset
Prediction of Attack
Send Normal Report
Detection of Attack
Category of Attack
Predication of Preventive Action
Providing Security
Storing Result for future use

Figure 2: Flow of proposed work

The collaborative framework is conceptually composed of three essential elements, a detection engine that is local to the system, a collaborative ML engine, and a pre-processing engine that preserves privacy. The collection and pre-processing of data from the VANET framework take place in the pre-processing engine which determines the activities of the vehicle system in real-time and help to secure from unauthorized access.

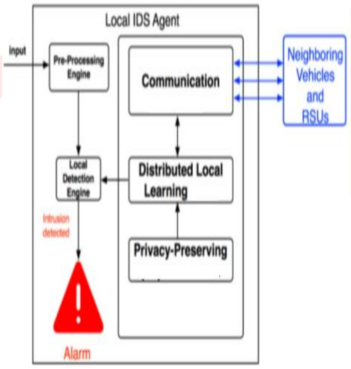

Figure 03: Architecture of Proposed IDS System using ML

3.1 Mathematical Model:

To provide a mathematical model of our suggested AV scheme, hear uses the different parameters. With this we can secure the AV communication with maximum throughput, Accuracy & minimum packet drop probabilities:

$$a\,(s,n,t,r,d) = t \,.\, c\,(s,n,t,r,d)$$

where,

s: source node (Vehicle)

d: destination node (Vehicle)

n : total number of node in network

r: range of particular network in which node to node communication can be possible

a: Resultant malicious node detection parameter,

c: Cooperative malicious node detection scheme,

t: Improvisation factor that is based on probability $t = (P^{load} + P^{mobility})\ /2$ where P is probability

load: total number of nodes which perform communication between node to node.

Mobility: Movement of node or speed of node in particular network

By using the above model, we are trying to find the misbehaving activity in-network with proper or secure communication between the AV.

IV. Result & Discussion:

The assault on a DDoS is an effort to make a website or online service unavailable by overloading it from various outlets with large traffic flows [13].

Unlike a Denial of Service (DoS) attack, which uses a computer and an Internet connection to inundate a single resource with packets, a DDoS attack uses several computers and Internet connections frequently distributed worldwide by a botnet. A massive volumetric DDoS attack can produce tens of gigabits of traffic per second (and hundreds even of Gigabits).

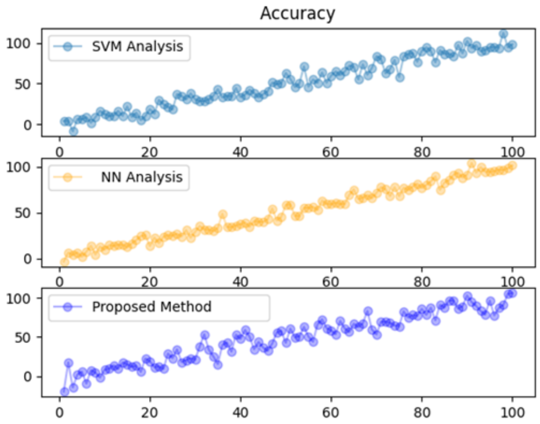

Figure 4: Accuracy of the proposed model with existing some basic approach

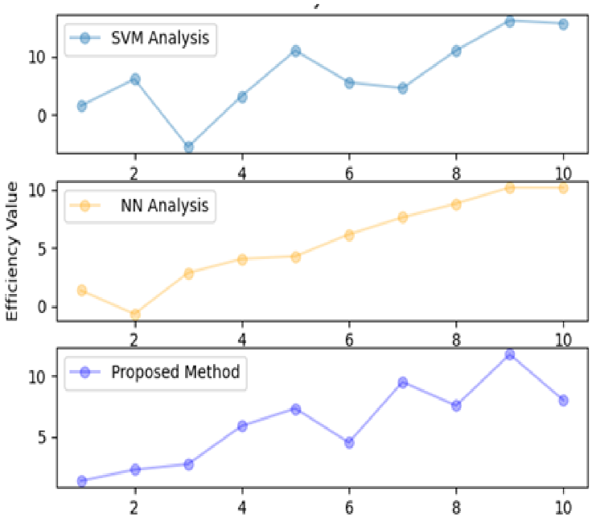

Figure 05: Efficiency using CNN, SVM & Proposed Approach

The above figure gives a detailed overview of the proposed approach with existing it shows that it gives better accuracy using the hybrid approach as compare to others.

V. CONCLUSION

As cars get smarter, scientists need to prevent cyber attacks. In the experiment conducted, the network is jammed, and receiving nodes lose messages from the benign host as the period reduces and the number of jammers increases. The most common forms of cyber threats are DDoS, Eavesdropping, Man-in-the-Centre. As we introduced the AV contact channel to our DDOS attack experiment. The performance analysis of the proposed hybrid approach gives better accuracy as compared to others. In the future, real-time CAN experiments must be conducted to better assess the effects of these cyber-attacks (Controller Area Network). Such cybersecurity techniques are the key strategy for stopping such penetration tests. As well we can test the working system with other ML approaches and parameters to know the more accurate result analysis.

REFERENCES:

[1] H. Ye, L. Liang, G. Y. Li, J. Kim, L. Lu, and M. Wu, “Machine Learning for Vehicular Networks: Recent Advances and Application Examples,” IEEE Veh. Technol. Mag., vol. 13, no. 2, pp. 94–101, 2018.

[2] Stefan Mihai, Nedzhmi Dokuz, Meer Saqib Ali, Purav Shah, and Ramona Trestian, “Security Aspects of Communications in VANETs”, 978-1-7281-5611-8/20/$31.00 c 2020 IEEE.

[3] Fabio Gonc alves, Bruno Ribeiro, Oscar Gama,“A Systematic Review on Intelligent Intrusion Detection Systems for VANETs”, 978-1-7281-5764-1/19/$31.00 ©2019 IEEE.

[4] MA Hossain, RM Noor, KLA Yau, SR Azzuhri, MR Z’aba, I Ahmedy,“Faster Convergence of Q-Learning in Cognitive Radio-VANET Scenario”, 78054-78108, IEEE2020.

[5] WANG TONG, AZHAR HUSSAIN , WANG XI BO , AND SABITA MAHARJAN , “Artificial Intelligence for Vehicle-to-Everything: a Survey”, 2169-3536 (c) 2019 IEEE.

[6] Carlos H. O. O. Quevedo, Ana M. B. C. Quevedo, Ahmed Serrhouchni , “An Intelligent Mechanism for Sybil Attacks Detection in VANETs”, 978-1-7281-5089-5/20/$31.00 ©2020 IEEE.

[7] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, “Artificial Intelligence for Vehicle-to-Everything: A Survey,” IEEE Access, vol. 7, pp. 10823–10843, 2019.

[8] A. Kreetzer, "The Connected Haven," 2017. [Online]. Available: http://visions.newmobility.global/0817/faye-francy-auto-isac.

[9] V. Haydin, "The Emerging Future of Autonomous Vehicles | Intellias Blog," 2017. [Online]. Available: https://www.intellias.com/the-emergingfuture-of-autonomus-driving/.

[10] B. Howard, "Fatal Arizona Crash: Uber Car Saw Woman, Called It a False Positive," 2018. [Online]. Available: https://www.extremetech.com/extreme/268915-fatal-arizona-crashubercar-saw-woman-called-it-a-false-positive.

[11] Atul B Kathole, Dr.Dinesh N.Chaudhari, “Pros & Cons of Machine learning and Security Methods ”, 2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588,Volume 21 Issue 4

[12] Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, “ Machine Learning & its Classification Techniques ”,International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.

[13]Atul B Kathole, Dr.Dinesh N.Chaudhari, “ Fuel Analysis and Distance Predication using Machine learning”, 2019 ,International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 5 Issue: 6.

[14] L. V. Anderson, "What To Read About Uberś Ùnquestionable Failure΄In Arizona," 2018. [Online]. Available: http://digg.com/2018/uber-crashanalysis.

[15] M. d. Cava, "Top robotics expert on Uber crash questions whether sensors worked," Mar 2018. [Online]. Available: https://www.usatoday.com/story/tech/2018/03/23/top-robotics-expertuber-crash-questions-whether-sensors-worked/451420002/.

[16] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of computer security, vol. 15, pp. 39-68, 2007.

[17] P. Asuquo, H. Cruickshank, J. Morley, C. P. A. Ogah, A. Lei, W. Hathal, S. Bao and Z. Sun, "Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges and Countermeasures," IEEE Internet of Things Journal, 2018.

[18] M. N. Mejri, J. Ben-Othman and M. Hamdi, "Survey on VANET security challenges and possible cryptographic

solutions," Vehicular Communications, vol. 1, pp. 53-66, 2014.

[19] M. T. Garip, M. E. Gursoy, P. Reiher and M. Gerla, "Congestion attacks to autonomous cars using vehicular botnets," in NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA, 2015.