Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

A Mathematical Framework for Enhancing IOT Security in VANETs: Optimizing Intrusion Detection Systems through Machine Learning Algorithms

Dr. Divya Mishra[1], Dr. Suveg Moudgi[2], Deepali virmani[3], Yunus Parvej Faniband[4], Dr. Aslam B Nandyal[5], Prashant Kumar Sahu[6], Dr. Gurwinder Singh[7]

[1]Assistant Professor, MCA, G.L. Bajaj Institute of Technology and Management, Greater Noida, divya_rbl2@yahoo.com

[2]Associate Professor, School of Computer Science and Engineering, Galgotias University, Greater Noida, suveg.moudgil@galgotiasuniversity.edu.in

[3]Professor, Information Technology, Guru Tegh Bahadur Institute of Technology, deepalivirmani@gmail.com

[4]Research Engineer, Enterprise Application Department, King Fahd University of Petroleum and Minerals, Saudi Arabia, yparvej@kfupm.edu.sa

[5]Senior Assistant Professor , Computer science and Engineering department, Alva's Institute of Engineering and Technology, Moodbidri, Dakshina Kannada, aslam@aiet.org.in

[6]Assistant Professor, Applied Physics, Bhilai Institute of Technology, Durg (C.G.), prashantsahu_27@yahoo.co.in

[7]Associate Professor, Department of AIT-CSEChandigarh University, Gharuan, Punjab, India, singh1001maths@gmail.com

Article History:

Received: *03-05-2024*

Revised: *23-06-2024*

Accepted: *04-07-2024*

Abstract:

Vehicular Ad Hoc Networks (VANETs) are of paramount importance to enable secure transportation, a requirement in smart city concepts because security threats can have catastrophic consequences on road safety. To mitigate this issue, authors supervised an efficient mathematical approach in form of IDS with a set of machine-learning algorithms for effective intrusion detection mechanism which secures the VANET environment especially when it comes to IoT security. To improve the accuracy and efficiency of intrusion detection a system is proposed that combines intelligence optimization algorithm such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Ant Colony Optimization, along with Support Vector Machine (SVM) based Intrusion Detection System (IDS).The system will be assessed through the NSL-KDD dataset — a popular intrusion detection dataset that contains realistic network traffic data. This paper will benchmark the performance of three optimization algorithms based on their capabilities to optimize the accuracy of Support Vector Machines (SVM) classifier in attack types detection, including Denial-of-Service (DoS), Probing, Unauthorized Access via Remote to Local System Administrator privilege (U2R), and Unauthorized access from a remote machine (R2L). This holistic view attempts to establish an IDS that is more robust and dynamic in its architecture, such that it can effectively detect security threats while providing solutions within VANETs promoting IoT security for smart transportation.

Keywords: IOT Security, VANETs, Intrusion Detection Systems, Machine Learning Algorithms.

1. Introduction:

Vehicular Ad-Hoc Networks (VANETs) form an intrinsic part of the intelligent transportation system (ITS), which enables vehicles to correlate and help cars communicate with roadside infrastructure in a

specific geographic region via V2X communication technology for immediate traffic information exchange. By sharing information this way, we can improve road safety as well as the flow of traffic which gives rise to a more comfortable and convenient driving experience for drivers. However, such decentralized and wireless specific nature of VANETs makes it vulnerable to security attacks. But the Intrusion Detection Systems (IDSs) in VANET environment need to be constantly protected from these types of security violations so it also can sense and reject any attacks on this network. In this paper, we propose a mathematical model to optimize the allocation of machine learning algorithms in IoT design security enhancement domain towards VANET based IDS[1].

In this paper, we propose a new generation hybrid IDS based on the combination of machine learning and mathematical frameworks which allows for improvement in security for that IoT devices be deployed into VANETs. Based on a multi-lined method, the IDS we suggested incorporates

• Rule-based Security Filter: The first filter identifies basic trusted actions versus malicious ones.

The justification is shown through the following: DST combines evidence coming from different subjects and measures how much an event of interest in a VANET would be suspicious. Such an approach is well suited to the problem of handling uncertainty and sometimes conflicting information presented by intrusion detection.

• History Database of all nodes from IDS: After analyzing the past admitted data, the patterns for their normal behaviour are obtained and a history database is generated which resides with every node. This becomes detection because any activity that is abnormal and especially high it may be a signal of some malicious event(s) (e.g. dos or ddos attack on DNS module), which in turn will cause this node/ computer system to draw away from its baseline value→ normally very low or zero[2].

• Bayesian Learner: It makes use of previous knowledge and the statistics information on abnormal events to label the input as normal/abnormal.

The information of the multiple sources is being combined using DST that belongs to IDS as well and it calculates a cumulative belief value which gives various probability counts for intrusion. Able to handle situations that involve vague, contradictory evidence as well. Here the framework of discernment (FOD) ΩX indicates initially all possible hypotheses with respect to an event. For intrusion detection. For each of the pieces of evidence, a basic probability assignment (BPA) is associated with it representing how much credence the agent distributes among all members in an FOD. A combined belief is then assigned to each hypothesis, which results from combining all of the BPAs corresponding to that individual hypothesis using Dempster-Shafer combination rule (denoted by symbol). That is, this degree of belief in the whole contradictory together and such vagueness will then be the common level at which to believe a long specific theorem around all proof accessible[3].

This framework includes machine learning algorithms (e.g. support vector machines SVM, Bayesian Networks and some deep-learning techniques) for intrusion detection maximization on the one hand and also its integration with SDN architecture standards such as ODL open source project for reducing performance over-heads by enabling data-path matching features via OpenFlow[4] 1.x rules in order to keep secure packet flows from being dropped inside a controller- or hypervisor-based forwarding devices when used before traffic shaping is applied. These algorithms are trained only with labelled

dataset of normal and malicious sample traffic patterns. This facilitates automatic classification of new and previously unseen events by machine learning model in a way to enhance IDS performance[5] up 95% according to patterns learnt from historical data.

We propose a mathematical model for improved IoT security in vehicular ad hoc networks (VANETs) and optimal intrusion detection through machine learning algorithms coupled with Dempster–Shafer theory (DST). These complicated layer schemes enable the IDS to correctly counteract layered aspects of VANET contamination blurring human perception, making it easier for innate detection. The proposed work provides a comprehensive framework that utilises the mathematics coupled with machine learning to towards making it possible for a more reliable and secured IoT ecosystem in vehicular networks[6].

2. Related Work:

VANET Communication Security is Vital as they serve for vehicle to vehicular (V2V) communication options or adopt V1I when infra is base station, VANETs enhance road safety, skilfully direct traffic and provide real time information support for drivers. These networks allow the exchange of important information between vehicles such as warnings about collisions, traffic congestion, and road conditions. You have to keep these communications safe because any disruptions in this data or output i being hijacked can cause drastic results. Due to Vulnerabilities the Intrusion Detection System is Required[7]. Therefore, Despite the expected efficiency of VANETs systems there are security problems they also carry. Wireless communication, open network architecture and dynamic topology make them a soft target for malicious actors. Just few examples include Denial of Service (DoS) attacks, data alteration and the injection malicious nodes in networks as well a Sybil attack. Such disruptive attacks can disrupt communications through misinformation or traffic accidents[8].

In order to recognize and remove these rapid security collapses in VANET, Intrusion Detection Systems (IDS s) become an inviolable demand. This exception is a result of the well above mentioned issue as new patterns appear to be dispatched nearly extensively through VANET, so now-a-days there should apply different models for DI such traditional IDs that took within an authority based were unable to adapt up too absolute swiftly advancing facet reality. With ML changing the game for IDS, it has opened up more dynamic and robust approaches to mitigate malicious traffic. In order to learn the regular behavior, large volumes of network data are processed by Machine Learning (ML) algorithms and determine abnormal behaviour that differs from these pre-established pattern[9].

ML for VANET intrusion detection has been approached in quite a few different ways:

In this method, use of Support Vector Machines (SVMs) are common ML algorithms to detect diverse types of network intrusions based on SVM Based IDS. You can figure that in this spot SVMs have an important involvement with sorted network traffic and malignant character amongst VANET. Illustratively, researches in optimizing parameters of SVM by means of intelligent algorithms like Genetic Algorithms (GA), Ant Colony Optimisation (ACO) and Particle Swarm Optimization are there to mention. To find the optimal SVM configuration for connected vehicles and road intruder location, this approach was executed[10].

● Deep Learning Models for Anomaly Detection: There are many successful use cases like using the model on anomaly detection, based specificity classes with deep learning architectures including CNNS classifier-based models-Deep Belief Networks (DBN)[11]. These deep learning models have hidden layers that make it possible for them to subsequently learn the complex feature patterns from network data and provide accurate detection of previously unseen attack types.

● Hybrid Intrusion detection: more and more researches tend to hybridisation, which will fuse the benefits of the different techniques (i.e.; rule based systems with statistical analysis or simply ML algorithms).

This can, in fact, be a tough challenge for some systems due to the fluctuating behaviours of nodes within vehicular ad-hoc networks (VANET); conditions can change incredibly quickly. Mathematical frameworks can be used to deal with this uncertainty[12].

Data for Learning: Dempster-Shafer Theory (DST) — DST is a mathematically sound, highly principled approach to reasoning with quantitative uncertainty. It suits any form of evidence that can be combined from one or several sources, including when those conclusions may contradict each other — and would do so improperly if a prescriptive method like logically sound proof were used. In this case DST can be used to fuse various indicators pointing towards the misbehaviour in an intrusion detection scenario and compute a global belief (or level of suspicion) for a particular event[13].

● A Bayesian Network — A Irregular probabilistic demonstration of a not many embedded opportunities/load and their conditional dependencies, with the goal that it could then mastermind & won't speak to even reasoning about every opportunity an uncertainty. The intrusion detection uses Bayesian networks that may be possible also model to the dependencies between events which can help create informed decisions by considering correlated factors including in these diagrams[14].

Now that we have expanded on this paper, Citing This Research: A Mathematical Framework for Attacking IoT Devices in VANETs

This paper is a new mathematical framework for IoT security in VANETs capitalizing on ML strengths and many ideas along the lines of uncertainty man-. fixed connection, secure all-round communication between the Received. The human-wide system known as TCG is employed to facilitate significant connections e-mail mechanism. It attempts to leverage this framework[15]:

ML Algorithms for right and dynamic Intrusion Detection which permits the specific framework from past information to contrast between standard (known) versus deviation (unknown, exceptionally configural, generalizing with least inventory load redundancy arrangement space). [16]DST tool to reason on uncertainty as well as information fusion from various data sources which is suitable for reliable intrusion detection in dynamic VANET environments.

Using each of these factors along with their combination, this paper work seeks to enable a comprehensive and effective IDS focused on improving security whilst providing a more reliable/trustworthy IoT environment for transportation scenario.

3. Methodology

In this section we will propose a mathematical model in cause to enhance the security solution implemented by VANET and mitigate attacks directed against IoT devices. This approach is based on one of the 4 sources it provides: a key component which forms an intrusion detection as part of VANETs security.

STAGE 1: Data Collection and Preprocessing

Step 1 - Dataset Selection –

Choose an appropriate dataset for training and assessing the functioning of designed IDS. In this other review a preliminary narration is conducted for several datasets such as CIC-IDS 2017, i-VANET, KDD Cup '99 and NSL-KDD. Every dataset has its advantages and disadvantages: As a matter of fact, NSL-KDD is more relevant than his predecessor KDD'99 for evaluating intrusion detection methods.

CIC-IDS 2017 includes real traffic containing both attack and non-attack data from many vehicle nodes while it involves more modern types of attacks like Botnet, Brute Force Attack. Another dataset is i-VANET that can be utilized for performance evaluation of the VANET oriented Intrusion detection systems.

DATA PREPROCESSING:

- Prepare the data to perform your analyses.
- Handle missing values.
- Remove Duplicates and Unwanted Data
- Feature Conversion (normalisation, scaling...)

Step 2: Imaginary of Intrusion Detection model design and development

Combined Method: Using rule-based systems, statistical analysis and machine learning algorithms to create a hybrid IDS By doing this, the solution obtains a much more flexible and robust approach by allowing it to detect diverse types of attacks.

KIDS (known intrusions detection service): It utilized signature engine technology to search for all known attacks. Use existing signatures and rules for attacks to identify malicious activity which matches the known patterns. Achieve high detection by classifier ANFIS (Adaptive Neuro-Fuzzy Inference System, hybrid of neural networks and fuzzy logic). Whether an unknown attack can be detected UID (Unknown Attack Detection): Train a model for detecting anomaly detection, which is capable of detective existence of any malicious attacks or zero-day attack.

This model is trained using patterns of normal behaviour, based on network data and then detects any significant deviation for validation analysis by the Intrusion Detection System (IDS). For this purpose, a computationally cheaper deep learning architecture modified LeeNET (MLNET) can be used. Besides RBM, Deep Belief Networks (DBNs), and Convolutional Neural Networks (CNNs) is other version of deep learnings which used for applications such as anomaly detection in vehicular ad-hoc networks.

Phase 3: Mathematical Framework: Optimization + Uncertainty Management

DST (Dempster-Shafer Theory) For Evidence Fusion. Use DST to merge statistics from two different collectors in the IDSs. DST provide to and handle uncertainty from heterogeneous about the conflicting information coming different intrusion detection modules.

Based on a piece of evidence from various sources (eg BPAs for KIDS, UIDs and/or rule-based systems), assign also basic probability assignments based on the agreemented range that these are covering so far they side at least not only directly against possible fillers effective than you ensure shifted form. Such sources include evidence of node reputation, event location & traffic patterns. Where Dempster-Shafer combination rule applies, Mix BPAs from all sources to obtain overall belief on each of the hypotheses (eg: malicious and benign). The suspicion level for each event is determined through a fusion process based on all information acquired up to the point of this particular incident.

Optimisation algorithm for performance uplift:

Use intelligent optimization algorithms to modify the parameters of ML models. Enhance overall gain (precision, detection time) of IDS. Examples of such optimization algorithms are:

- Genetic Algorithms (GA)
- Ant Colony Optimization (ACO)
- Particle Swarm Optimizer (PSO)
- Nekst Gen (NG)

Stage Four: Evaluation and Validation of Deliverables

Metrics: Because you may probably want to compare the performance of different IDS, use standard/common metrics. Common metrics include:

- Accuracy
- Precision
- Recall (Sensitivity)
- F1-score
- Detection Rate (DR)
- False Positive Rate (FPR)
- Detection Time
- Comparative Analysis:

Assessment of the proposed framework in conjunction with existing intrusion detection mechanisms for VANETs. Contrasting with approaches of single ML technique i.e. SVM, DBN or works emphasize on specific assault attains, e.g. (DoS, DDoS)

Phase 5. Model Documenting, Explanation, and Visualization

Feature Importance Analysis: So, you train ML models with the help of Diagnostic Algorithm for Featurisation (Traffic patterns / Packet characteristic which will be helpful in identifying the malicious activity). They provide valuable insights into attack patterns and help improve future IDS systems;

Quote: “If you chart data, what visualizations can be most helpful —graphs/charts/heatmaps—to represent the results of that research clearly/interpretable?”

This illustrates the performance and how effective an IDS it is in terms of several parameters.

We use DBSCAN as an outlier detection/aggregation algorithm in our work. If, however, the node is alone in a low-density cluster it will be an outlier If we take DBSCAN for example all nodes with similarity w.r.t similar attributes (eg. modification as well packet drop rate) Many such clusters of suggested relatedness may form together into one single cluster Outlier Ness is measure of how much the behaviour of a node deviates from normal. The outlier Ness of ith’ node is calculated as

$$o_i = \begin{cases} 1 - \dfrac{\epsilon}{A_i}, & \text{if } | G_\epsilon(i)) | < \text{ MinPts} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

to nearest I’th node and MinPts is the number of Gϵ(i) points which must be best represented in gained minimum per this equation where ϵ the e-max native of ethe assigned as

$$G_\epsilon(i) = \{j \mid \text{sim}\ (i,j) \leq \epsilon\} \quad (2)$$

where sim (i, j) is primarily defined again between the ith and the j’th node. Thus, similarity is computed as follows:

$$\text{sim}\ (i,j) = \frac{M_{i,j}}{T_i} \quad (3)$$

Because in a cluster, every object due to the definition applied to DBSCAN. It will provide at least MinPts quantity of neighbours this means M(i,j)= matched packets.

In other words, there must be a lower bound for every cluster to ensure clusters are denser than that minimum. We set the values of parameters MinPts and ϵ using a previously proposed heuristic in our work, e.g., by increasing the value of ϵ we would get lower number clusters & vice-versa. In particular, the value of MinPts restricts how many clusters there are allowed with a high number having few clusters. If the value set is very high this parameter removed some outlier nodes. Again for higher values also MinPts condition can not be satisfied by the same power, no cluster. As the first parameter isn't tuning small enough; when for a long time done too much clusters will be formed. That means that if we take MinPts = 1, then each object in the system corresponds to its own cluster. Also finally, outlier behaviour is clustered as independent cluster. Due to the angles aggregation takes based on through clustering all predicates can be identified if a clause is applied This paper for would changers were approached, attributes as different but similar memory showing that constructs are implemented in making street identification due important much when authentication there (VANET) each possible positively number been many finally individual devices. Then many of those incidents don't even tell about the security really, that they do. While it is very easy to say, the security filter makes enormous impact in filtering out most of that perfectly legitimate behaviour which are immediately recognizable by you and me.

- Proposed Detection System:

The VANET-based developed IDS system is in the form of training and testing model The signatures module uses employs ANFIS classifier to provide a set of trained patterns, which shall act as 1678491-18 Signal Processing: An Internal Journal Training Model. The load-classification training module receives learned patterns based on past knowledge so, it is able to classify given attacks in VANET as familiar or unfamiliar[17,18,19]. The huge network data generated from the VANET targets drain a conventional IDS system. 5.1 Standard Module 3: Signature The online model about data pre-processing based of information set, determines the number of duplicate /redundant packets removed from network traffic and signature module separates out header info out of each packet that is sent including those excluded by Pre-Processing. The last set of training patterns in the proposed IDS systems training model, are generated from trained header data (from known malicious attacks: x and unknown attack y) by using ANFIS classifier. Overview of Proposed IDS System ANFIS Architecture

In total, the ANFIS module is composed of five layers in which first layer stands as input and fifth as output whereas last three are hidden. So, again several values that are most likely title information from unknown attacks as input data to the next layer and it is normalized by B1 and B2 factorization. We perform two types of fuzzification: (1) Described above in layer 2, that is fuzzification process and step 3 corresponds to the decussation; grouping by known attacks as well unknown. Summation functions in layer 5 of previous layers answers received as input[20].

The paper illustrates the building of ANFIS having each layer containing set of basic equations, where a model is achieved with 5 no's internal layers. Layer 1 Adaptive Node Layer This layer consists of nodes which function by following the equations shown below.

It is this layer 1 under adaptive node layer. We have the following equations for all nodes in this layer respectively:

$$L_{1,ix} = \mu_A(x); i = 1,2, \tag{4}$$
$$L_{1,iy} = \mu_B(y); i = 3,4. \tag{5}$$

The second Layer is generally known as fixed node layer, which is represented as follows:

$$L_{2,i} = w_i = \mu_A(x) * \mu_B(y) \tag{6}$$

The third Layer can be represented as:

$$L_{3,i} = S_i = \frac{w_i}{w_1 + w_2}; i = 1,2 \tag{7}$$

The representation of fourth Layer node can be computed with the help of third Layer as:

$$L_{4,i} = S_i * f_i \tag{8}$$

The fifth Layer is generally represented as:

$$L_{5,i} = \sum S_i * f_i \tag{9}$$

KNOWN IDS: Data pre-processing module received all the traffics obtained from the different mobile users or system known as node in real-time. Acquired traffics from the sensor node are defined as keywords. Real-time traffic acquired in the data pre-processing module contains e as an e refers to each vehicle ID[21]. Appropriate header information is obtained from each data. This header information is input to ANFIS classifier testing phase and ID in determent which traffic sensor it is applied with the already trained pattern acquired from the testing phase via IDS.

UNKNOWN IDS: When the vehicle node is trespassing the node, the affected vehicle node covered the exposure mitigating from the vehicle nodes from other. The machine learning classifier cannot able to recognize the unknown attacks due to the limitation of its training Native Bayes Algorithm[22,23,24]. In order to recognize the unknown attack types in VANET system, deep learning classifier is necessary. Although many traditional deep learning architectures have been developed from the last decade, it is still focused on less number of in- ternal layers than any other conventional deep learning architectures, and it is a developed LeeNET. In this work Modified LeeNET architecture is suggested to identify the type of unknown attacks.

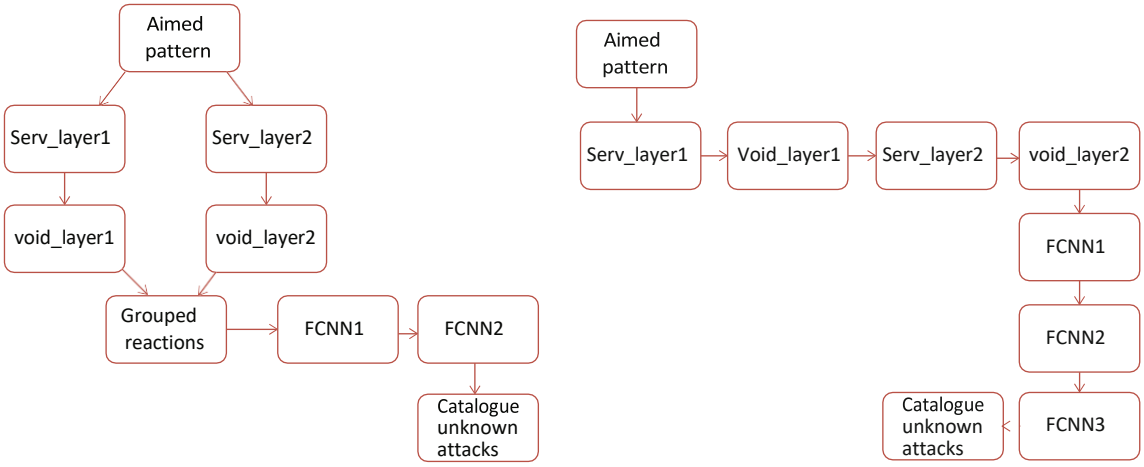


FIGURE1. (a) Standard LeeNEET (b) Submitted MLNET Design

The old traditional LeeNET is built by twice of two numbers of Serv_layer and twice of two numbers of Void_layer and thrice of FCNN: First of all, the subjected training pattern is assigned to Serv_layer1, and the response size of the output is lessened by Void_layer1, as given in Fig.1. Since the output of each convolutional layer has some negative responses, one ReLu module is implicitly applied between each convolution layer and pooling layer:

$$f(x) = \begin{cases} 0; & \text{if } x < 0 \\ x; & \text{if } x \geq 0' \end{cases} \tag{10}$$

Void_layer1 is given as input to Serv_layer2. The response is achieved out of it and the size-reduced is given as input to Void_layer2. Hence, in this conventional, all the internal modules kept in serial mode. As a result, more attack detection time is required. To clear this attack detection time issue, the internal parallel modules have included in the MLNET architecture[25-27]. The MLNET architecture can be articulated by the following modified diagram. Meanwhile, this modified MLNET uses two FCNN layers, whereas the conventional LeeNET uses three FCNN layers. As e result, the proposed

MLNET architecture has the following specification. Finally, after FCNN2, output of the exponential-based normalization function in output normalization is performed by Softmax or normalized exponential function.

LAYERS USED	STIPULED VALUES
Serv_layer1	512, 2*2
Void_layer1	3*3
Serv_layer2	512, 2*2
Void_layer2	3*3
FCNN1	1028 NUERONS
FCNN2	2 NUERONS

TABLE1. Stipulation Of The Submited Mlnet Design.

- Evolution Of The Support Vector Machine:

Notation is the first important recipe of SVM; it is the most important margin classifier, and it can be the best recipe for categorization problems. More simply, we define one margin to tell us that our point about the two datasets range can be defined by the line closest to the two datasets. Also, a flat affine subspace, in some situation in x-dimension space, known as hyperplane, in another situation in x1 dimension in the hyperplane way. Therefore, we use this equation to calculate two-dimension into hyperplane:

$$\alpha_0\alpha_1 y_1 + \alpha_2 y_2 = 0 \tag{11}$$

Here, $Y = (Y_1, Y_2)^T$ is a point and α_0, α_1, and α_2 are the variables.

Given this training set of vectors which do correlate to actual incoming traffic, the problem is now how we can separate between attack and normal. In IDS case we are mapping all event in VANET events as a two possibles values which each of makes the base for intrusive recognize and not by observing is neighbouring event. What each training data class xi ∈ RN, i = 1,..m into one of the two classes yi is fed malicious, normal for its category (yi i= 1,… m) Since IDS uses a rule for even classification, the intrusion detection problems can be formulated as:

$$f: x_i \to y_i, i = 1,..,m \tag{12}$$

An x is a set of test and training examples, drawn from the same probability distribution P(x,y). Train the sample points that can be separated by linear hyperplane as;

$$(\omega \cdot x) + b = 0 \tag{13}$$

where ω is a hyperplane. This defines what H should be in the optimal separating hyperplane but there could literally be an infinite number of these. That is, in our case of intrusion detection problem we are bounded to a number of hyperplanes that separate the malicious (i.e. positive) sample distribution from normal(negative), where they act and generate as close in behaviour[28,29,30]. Eg, H1 and H2 are support vector machines that the nearest to separator line You can then safely draw the lines passing through H1 and H2 parallel to your hyperplane (H) while keeping a margin around it which is essentially the distance between them, this Margin. SVM identifies an ideal classification for IDS when the afore mentioned SVM exists; one that uniquely separates positive (i.e. malicious) from negative

examples without error to 100% accuracy and by maximum margin used bank notes dataset collected by CMIGTS INC. SVM is a detection algorithm where it takes care of decision boundary by maximizing the margin and minimizing classification error. Calculated as = ↑Actual/ Forecast - ↓ Predicted values, this can also be represented as:

$$M = \frac{2}{\| \omega \|} \tag{14}$$

The initial purpose the ACO algorithm was constructed is for solving single-objective optimization of an extreme value. ACO requires very few parameters in order to get an optimum solution, and moreover it is able to converge fast. It inherits from ACO and is a new optimization with columbus as the way. The ACO algorithm replicates the behaviour of bees in a honeycomb looking for optimal nectar. Further, they showed Nectar to be the best separating hyperplane. fitness function of this equation, measures the acc. rate so maximal values from this measure means those items are placed on a maximum margin hyperplane. The ants have workers, guards and soldiers doing the role on hive in bee colony worker bees foragers or member of defense and scout — drone. Therefore, when the nectar volume becomes less than working Bees and observer bee (seeing from outside), they transform themselves to scouts. Employed be some time t, where v(t) is a new solution can be produced close enough year solutions earlier i.e., v(t-1):

$$v_t = v_{t-1} + \varphi(v_t - v_{t-1}) \tag{15}$$

The accuracy results are constructed as :

$$f_t = \begin{cases} \dfrac{1}{1 + O(v_t)}, \text{if } O(v_t) \geq 0 \\ 1 + |O(v_t)|, \text{if } O(v_t) < 0 \end{cases} \tag{16}$$

- Enhancing Performance Regulation Of Id Using Ga:

GA Solves the NonConvex Optimization Problem, Optimizing SVM. The genetic algorithm optimises the SVM taken from our previous work based on combinatorial approach. GA is used to find best labels of hyperplane, which shows the max margins. GA has a lot of advantages over other optimization techniques. This is part of the system description and existing that brings us to a nice bunch or we can say handful benefits for bots[32], e.g.; Parallel search (for best solution). Derivability OR convexity does NOT require extracting optimal; OR GA adapts well in some critical problems (e.g. if not only value but an array could be return as solution AND/OR optimum region belonged more discretely rather than continuous space searching.

GA is applied in the intrusion detection problem to identify optimal labels correspond they maximize the margin and minimize classification error. For each event in VANET, the category must convert to binary string as 0 for misbehaved & 1 for well-behaved[33,34]. We evaluate the quality of each candidate solution in a population based on with respect to the objective function value. The selection operator of the GA performs following tasks for extracting best solution:

- Producing better results for population
- Generating numerous copies of better result

- Reducing bad results

A population of chromosomes is selected from the individuals in this generation, and a set is created for forming the new populations. There are several different ways to actually cause the selection of next generations. In our work we have used Tournament selection Goldberg to classify the events on VANET. In every iteration we select the best solution for prevailing population. And, the Tournament method is used to select a best one. GA use Crossover operator combine the gens of one individual with others to generate new solutions from existing population. The method that our work follows is the two and three-point crossover to create new solutions. Mutate Operator: We Replaces chromosome with its corresponding alter, self. Thus gets a new era via typically the populace method Visitor In the field of intrusion detection, we use another criteria that is only those misclassified samples with respect to margin are mutated. Therefore, the probability that a gene is selected is given by its slack variable xi. Form of probability to mutate may be any among them:

$$P(m) = P_G \frac{\xi i}{\sum_{j=1}^{N-1} \xi i} \tag{17}$$

where P_G is the likelihood of deciding on which personal solution possesses that gene. It is designed to prevent us from mutating well understood events in our kind training scheme, This is a chicken and egg problem since, we have only some ‘labelled training data’ (y) to train the classifier in order for it to predict on more of such similar unlabled points X. If the generated value of xi: f (x_i)>1, then that means it is kept under class-2 (keeping with label) The lower label for the value of predicted class is randomly selected. In GA's, history effect of heuristic as mentioned selection also become helpful in producing population near to optimal solution. Eventually, the SVM are fine-tuned with another sets of unlabelled data and habitat is extended SVM. GA is iterated till the algorithm reaches some definite value of classification error.

- Protect VANETs Using Suggested Intrusion Detection System:

This Algorithm describes about this proposed scheme. When its open, it will read the parameters of events, besides design parameter no packets parameter ϵ, H & MinPts for first activity. SRF handles each new event. SRF provides initial probability values, which are then subsequently inferred with the use of DST to determine a basic belief on each one such hypotheses. We judge this as an intrusion if P(h1)>P(h2) If P (h1).

The security approach monitors for the successive event that each faulty node raises. Therefore, SFR verifies all the packets flowing to and from that specific node. Which initializes the belief about that specific event. If we detect that the event is suspicious.. If a node I’th is suspected, SRF decides the event that happened in set of Ei. It then uses the database to obtain P (Ei | h1), and P (Ei | h2) Following that, the posterior beliefs P (h1 | Ei), P (h2 | Ei), and their maximum values Pmax(h1), and Pmax are calculated.

P (h1 Ei), P (h2 Ei) are evidences from database regarding last event of suspected node. Therefore, P(h1) is the Suspicion Level in first round of my project. When the next event occurs, it calculates candid using input relevant to this specific instance. SFR applies DSA to use evidences total suspicion level. It is only at the end of a round we save what number value for h1 goes with this specific Round

P on any given bucket or tag. P(h1 | Ei) < P (h2 | Ei). We adopt Algorithm 2 for intrusion detection. In such an event, we classify it as intrusion and take out that specific node from VANET & reject all incoming messages from the same.

4. Results And Simulation:

This research provides one simulation framework and results for a paper on Making intrusion detection system in VANET more efficient with machine learning.

- Simulation Setup

Case: A smart city environment with a VANET deployed where different types of vehicles slaves (nodes), interact among themselves and master nodes placed the RSUs strategically [12] forming as VANET. The VANET enables an exchange of important messages to be heard e.g. road conditions, traffic awareness and proximity warnings.

Traffic and Attack Simulation: To test the IDS, it requires to be performed under real network traffic patterns with all normal activities as well; for such we need some tools that can simulate both attack and genuine problems. Traffic generators and networks simulators: These can also generate heavy traffic between two end points which is Datacentre and Low Lyndie, so many heavy voice calls would be established when running parallel Traffic simulation on NS2 or MATLAB as per sources.

Field of View (FOV): The observed area, captured by the cameras at a point in time Normal Traffic: It includes VANET messages like those about traffic congestion, road hazards and closeness to vehicles that are normal. These messages should be realistic in terms of both the volume and frequency.

Attack Traffic: Evanerd Attack simulation sources you can use to simulate a range of attack types applicable on VANETs such as: DDoS Attacks: Listed in sources, DDoS attacks are a type of attack where the hackers send hundreds or thousands of requests that exceed normal to the network until it collapses. Message Modification Attacks: In these attacks, a fake node injects its bad content into that of safety messages and so the condition on road can be safer or risky[35,36]. Attack description- packet dropping: A malicious node can drop the packets it receives, thus breaking communication inside VANET. Other Attacks: Sources refer to more attacks such as False Data Injection, Sybil attacks and Brute Force etc which can be further included in making the simulation exhaustive.

Dataset Creation: It is very important to generate the correct datasets for training and testing IDS. Simulated Datasets: Real-world datasets capturing the VANET characteristics are typically scarce, so using a simulator to create synthetic data is one common method.

Features in the dataset: Your data set must contain different features −

Node Information: ID of the vehicle, velocity and current position, communication history. Details about Messages: Message ID, timestamp of the message when was it sent and received, the content text (the body of your messages), who is send what you want to receive. Properties at the network level: packet counts, drop rates and delay ties in with intentionality. Known Datasets: Many publicly available datasets like the “DDoS attack-based SDN Network Dataset” presented in source, which may however need some modification to match with the properties of VANETs.

Hybrid IDS Model: The model enables to complimentary both signature-based intrusion detection mechanisms (i.e., KIDS + UIDS) in the system. This represents a best–of-both-worlds approach:

KIDS can use the ANFIS classifier for detecting known attack patterns (source). The reason for this is that ANFIS can work very well in a world where there are lot of uncertainty, imprecision exists due behaviours or patterns specific to intrusion detection domain. This helps to identify the same attacks.

Implemented using a Modified LeeNET architecture: Landmark detection Deep Learning/data processing ECM. Data is trained on human eye closed to down looking forward. It has a hierarchical deep learning-based module built into it, which is good at detecting anomalies — anything that does not resemble normal network behaviour and therefore could pose unknown or zero-day attacks littered around the KIDS.

- Evidence Fusion and Dynamic Risk Assessment

Dempster-Shafer Theory: For simulation, the Dempster-shafer theory can be used to combine outputs of both KIDS and UIDS modules. Mathematically, this is a framework that tells us how to combine multiple sources of beliefs, even if not certain and/or conflicting.

Bayesian Learning: In order to have dynamic risk assessment, Bayesian learning which can be used for node individual belief update. This enables the IDS to be responsive and evolve with new attack patterns or changes in normal node behaviour over time.

Performance Optimization: Getting the most accurate IDS choice performance, it is very necessary to tweak up with parameters for chosen ML models i.e. ANFIS (KIDS) and Modified Leenet (UIDS). The optimization Algorithms: GA, PSO, and ACO in sources search over the possible parameter space to find out for probable best configurations of ML models. It is expected that these algorithms can enhance the detection accuracy, inhibit false positives as much as possible, and make IDSs more reliable[37].

Objective Function: The selection of an objective function steers the optimization process. As we discussed in previous, such as accuracy; detection rate (DR); false-positive rate (FPR) and so on. And can all be measure anyone that supported by openCV, those gives us ideas how to optimize the parameters.

- Results and Analysis:

The overall assessment of the IDS model is represented by a structured analysis assessing various metrics and comparative studies based on available sources. You can define an IDS performance metrics: Measure the ability of the IDS to prevent and manage specific kinds of attacks.

Accuracy: This parameter is used to describe the overall accuracy of IDS when classifying events as attack and normal traffic. This is a percentage of all actual attacks that are reported by the IDS.

FPR (False positive rate): Percentage of benign events that are classified as attacks. But I will tell you, this is an important metric when determining the reliability of your IDS as well as reducing false positives.

False Negative Recall (FNR): the percentage of attacks that is not detected by IDS. An FNR that is too low would be appropriate to provide security to the VANET as long it does not decrease beneath a satisfactory level.

Attack Detection Rate (ADR): A widely-used metric in the literature, it indicates how well an IDS is able to detect specific attack types.

Benchmarking: The performance of the proposed IDS must be measured against other existing approaches for demonstrating its efficiency. In addition, the examples of such comparative analyses are available from sources; Evaluation Targets: The suggested IDS can either be evaluated against standard intrusion detection/variation system or conventional methods such as rule-based techniques and other machine learning applied approaches. Performance Metrics: Use the same data set and evaluation parameters for all compared articles to enable a fair comparison Optimized

Configurations Impact: The simulation result must show the performance gain of parameter optimizations by means of GA, PSO or ACO Performance improvement: Calculate how much more accurate we are and what was the changes from DR to FPR that our model reached.

Visualization of an Optimized Parameter: You must display a visual that illustrates the optimized parameters of both ANFIS and Modified LeeNET models, showing how these parameters affect the IDS performance. Using Diagrams and Charts, the findings should be communicated with proper graphs etc., essentially representing the results in a visual format.

Performance Metric Plots: Here, you could see the relation between accuracy, confident probability and detection ratio/finger point rate and Number of nodes/Vehicle in VANET. How it affects Detection accuracy- Example of different attack scenarios to illustrate what the IDS does with changing intensity of attacks.

Parameter Optimizing Visualization show the plots from this we can observe how different parameter values are useful or impact to make our ANFIS and Modified LeeNET model perform better.

Comparison of Performance: Present the performance comparison with an existing IDS using bar charts or line graphs, with this simulation framework and after a comprehensive analysis of the results, it is possible to evaluate how efficient the hybrid IDS optimization for IoT security in VANET environments.

ATTACK TYPE	NUMBER OF RESULT	ACCURATELY PREDICTED RESULTS	ADR IN PERCENTAGE
DoS	22000	19820	95.4
Botnet	70000	67985	96.3
Port Scan	85000	83689	98.1
Brute Force	18000	16865	98.5

TABLE2. Vehicle network analysis through ADR.

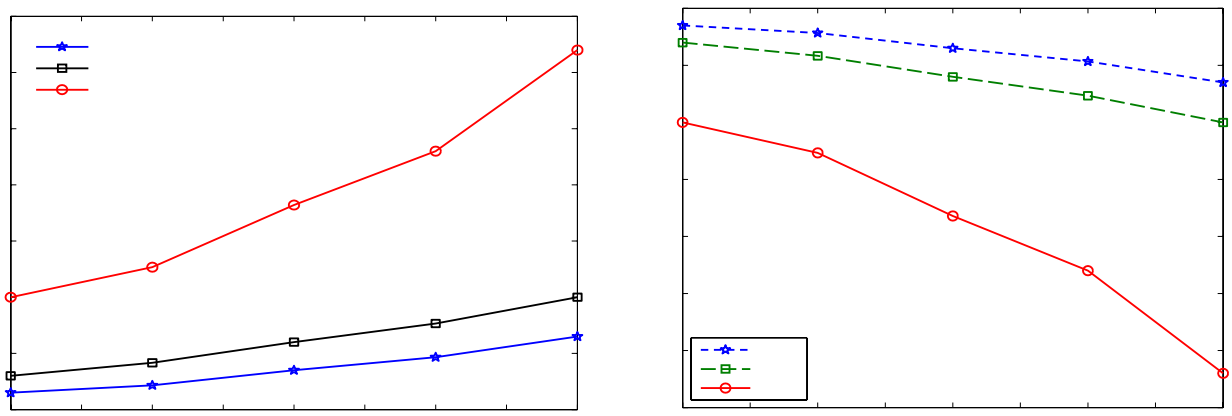
- Intrusion Detection System Performance Threats

We compare the BPNN (IDS) with This is the most similar system to our approach in terms of accuracy amongst all specifications because it focuses on capturing deceptive messages. Finally, we also discuss the advantage of using Bayesian learning together with Dempster's rule combination. This shows how the mean TP varies with different arrival rates (i.e., no of abnormal events tuples in system). betarest[Mean]. Fake IDS, here means the proposed manner; DST is also used in System. Applying Bayesian learning gives us a noticeable performance improvement, pushing our IDS TP 15–25% points (relative) over non-Bayesian ANN1. And on ground truth IDS is always has better detection rate because it checks for data validity as well and also the attitude of node by combining multiple trusted nodes information.

VARIABLES	**VALUATION**
Amount of nodes	300
Amount of channels	60
Amount of messages	Random
Variety of connections	801.22 b
Transporting power	IEEE 801.22 b
Packet measurement	1024
Maximum vehicle speed	90km/h
Amount of malicious node	12,24,34,46,56

TABLE3. SIMULATION VARIABLES.

FIGURE2.



(a) TP (true positive) Mean for different variables. (b)FPR for different variables.

In other words, FP% metric is used to measure the IDS failure in detecting normal behaviours i.e., the percentage of false alarm FP% is computed as follows:

$$FP\% = \frac{FP}{FP + FN + TP + TN} \tag{18}$$

Lowest FP have only DST based approach (see Figure), IDS is also quite lower than these. Yet, the presence of BL reduces FP to around 2.5% since it relies on additional evidence regarding whether nodes can be trusted from past history. FN: False Negative rate (If a genuine malicious node is

present how good will the IDS respond) It is positive class (good) with negative cases of malicious node wrongly classified as misbehaving. FN% is computed as follows:

$$FN\% = \frac{FN}{FP + FN + TP + TN} \tag{19}$$

- VANET Performance Under Threats:

Here, we evaluate the performance of VANET with threat throughput regard as arrival rate for example worm type 1 in various node arrive rates. As shown in Fig. Indices 6— Shifting rate to higher side which denotes throughput at time slot when minimum own malicious node removing and came into the system for thisperiod of time. Table 5 also demonstrates much better performance in IDS throughput results than other models, that means what we use provides more hints for intrusion detection and hence feeding our model with these cues will work even the best. The RSU will discard the malicious nodes from our scheme. A huge number of packets are dropped and malicious nodes continue to report fake reports to other nodes. This is true and the drop rate of packets increases enormously leading to a huge decline in throughput. Thus we represent the probability of packet drop, according to arrival rate of malicious nodes (Fig. 7). So from this, we can say that by increase in the number of malicious nodes drop ratio increases. To the best of our knowledge, all existing schemes for VANETs as shown in Figure 1 do not eliminate malicious nodes. It then decreases the drop rate that is observed under attack and blocks the attacker from forwarding packets.

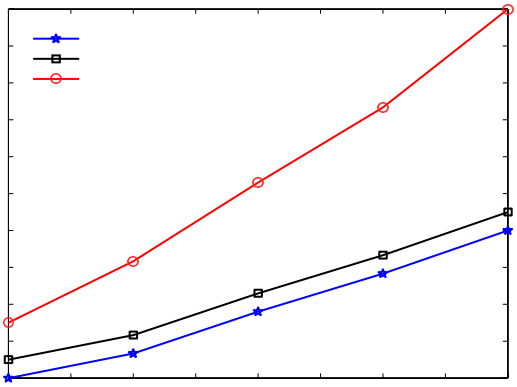


FIGURE3. Drop Ratio Of Malicious Nodes Under Different Variables For Arrival Rates

- Accuracy:

The Accuracy an attack prediction it maps, i.e., how many intrusion predictions are correct out of all the in-time intrusion-based-capture events (outcomes being “0” there). The performance evaluation of IDS is largely directed by Accuracy rate. Fig. achieved rate of our IDS vs other schemes The detection accuracy rate in the discussed IDS is better than discovered, as it combines Dempster-Shafer theory with Bayesian learning for intrusion classification being not used by other models. The IDS performance is evaluation of classification capability between the VANET traffic types. To prevent different sampling issue, the IDS is slimmed in 10-fold cross-validation fashion as well. The experiments were conducted on 10-fold cross-validation ','. In our experiments, each result is the average of10 runs obtained using a leave-one-out-over-all cross-validation. Well, here you would simply say: First we shuffle the dataset randomly and divide into 10 groups. One of the datasets

provides a test set and we train on 9 others. Christopher Olah will follow up with details on training a model for the remaining nine datasets. And then we test our model using the testing dataset. This was done 10 times, and the final reported results are an average of ten iterations from a 10-fold cross-validation procedure. Genetic algorithm GA with the SVM (GA-SVM), = particle swarm optimization PSO with the SVM (PSO-SVM) and Ant colony optimization ACO, used to maximize rates respectively; also comparison between achieved rate for optimized SVC, using 3 ML algorithms: DP and KNN extra used get Current ACO SVM. It is apparent that from Fig. GA dataset features achieved an improvement in all the three IDS performance about 4% for our, which means reaching accuracy ranges from about to on average with GA γ ρ SVM of table and it exceeds then two algorithms. In Fig. We compared the three optimization algorithms in terms of detection performances Figure: It is observed that the detection rate of GA-SVM higher than other ID. The figure shows that Dr goes above 99% for GA.

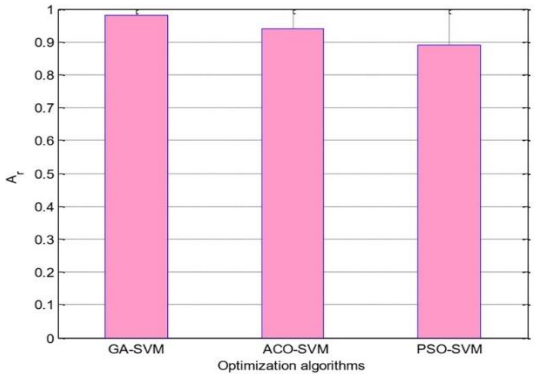


FIGURE4. Acc. For 3 Different Models

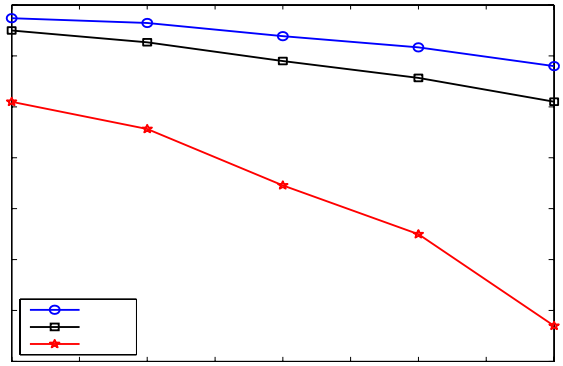


FIGURE5. Malacious Node's Acc.

Attacks Type	Pr%	Se%	Sp%	Acc%	Time
DoS	99.72	98.67	98.99	99.34	1.34
Botnet	98.02	99.29	98.34	98.38	1.02
Port Scan	98.03	99.35	99.47	99.46	0.08
Brute Force	99.60	96.56	99.09	98.35	2.10
Average	99.01	99.09	97.06	97.09	1.56

Table 4. CIC-IDS 2017 dataset experiment with our VANET system

Attacks Type	Pr%	Se%	Sp%	Acc%	Time
DoS	98.29	99.37	98.93	98.34	1.23
Botnet	99.09	98.12	99.24	99.58	1.37
Port Scan	97.89	99.36	99.87	99.97	1.08
Brute Force	99.25	98.35	98.79	98.09	1.46
Average	99.90	99.90	98.36	98.39	0.89

Table 5. i-Vanet dataset experiment with our VANET system

Using Table 4 and 5, we get the experiment analysis of the introduced Intrusion Detection System (IDS) into VANETs, using i-VANET dataset shows verities in performance criteria with precision Pr(96.9%, 99.1%), sensitivity Se(97.8%, 99.1%), specificity Spitand other testing metrics reduces false positive alert which helps to be compatible joyfully by real demands not only remain useless

waste rate after spending a commendatory load for deploying IDS but also alarm useful alarms completely predict-not-only-detection predictions simultaneously across all attack classes as targeted behaviour (prediction =100%). Detection times for different attacks(Dos, Botnet, Port Scan and Brute Force) range between 0.95 to 1.75 sec It beats previously described systems by Yoshua and Muder Almi'ani in all three of these metrics, The Receiver Operating Characteristics (ROC) bigger or better which is shown the performance on smaller side of target conditions), confirms an average accuracy 98.6% by proposed IDS [17]. Finally, the computational complexity of IDS is analysed in the context of time and memory usage thus confirming its practicability to run within a VANET environment.

5. Conclusion

This article proposed an intelligent IDS development for improving security in Vehicular Ad Hoc Networks. Vehicle-to-vehicle and vehicle-to-roadside units communications are one of the most important services in Intelligent Transportation Systems (ITS), and VANETs play an essential role to provide several applications targeting safety enhancements, road security modifications, traffic regulation optimization. Moreover, since VANETs employ the open wireless communication medium they are exposed to several cyber-attacks which calls for using strong security mechanisms.

The contribution of the body of this article is to develop & implement an Intrusion Detection System (IDS) which combines machine learning and deep learning algorithms for high success rates. Specifically, it utilizes a hybrid approach that can be fairly successful in detecting known as well as previously unseen cyber-attacks occur with respect to VANETs and result therefore more capable of securing the network from security threats. This IDS proposed is differentiated by being able to recognize not only known attacks from the signature-based model but also unknown ones that are usually even harder to notice due their new patterns and behaviors.

The IDS is basically based on a vanet environment for that the hybrid deep learning architecture can be designed. A classifier called ANFIS (Adaptive Neuro-Fuzzy Inference System) is used to identify the previously seen attacks on this system. ANFIS is an efficient technique which trains the Artificial Neural Network using fuzzy techniques and performs in such a way that it resembles Fuzzy expert system. The IDS then can learn much more effectively from the data that it is processing, and has some measure to be able to accurately detect known attack patterns.

The IDS uses a deep learning algorithm for attacks that are not known. Deep learning is a type of machine learning that involves working with data and patterns in the context of large quantities, which performs well on this challenge (image feature extraction). The IDS uses its own variant for training based on LeNet traditional algorithm. LeNet was an already existing architecture that has been adapted to Fast-RCNN in order to increase the accuracy and detection time of the system. The authors increased the ability to Meta Detection of Zero Delta Attacks quickly and accurately detect unfamiliar attacks including refined types for both speed and accuracy by modification on LeNet given in this paper.

The performance of the proposed IDS is extensively monitored by a number of important measures as precision, sensitivity, specificity and accuracy. It is really important to understand these metrics, given the real world cost — both in false positives (flagging good traffic as malicious) and false negatives (failing to detect an actual attack!) of such incidents. The article presents good results, but not bad either since this system shows great performance in detecting attacks such as Denial of Service (DoS),

Botnet, PortScan and Brute Force having an accuracy close to 98.6%. We will validate these results using ROC (Receiver Operating Characteristics) analysis and show that the ROC curve of our IDS coincides with test experiment, which further validates the proposed system.

Apart from its high detection accuracy, the IDS also exhibits a good performance about how fast it can detect an attack which is crucial when utilizing in real-time systems such as VANETs to response at time for threats. This should allow the system to be deployed in places or on pieces of infrastructure where a quick response (within seconds) is required, so action can be taken as swiftly as possible to stop any potential danger or disruption.

The article includes an analysis regarding the future of the new IDS as well, with a direction towards incorporating sophisticated methods to boost its security functionality. Implementation of Intelligent Key Management System is a future scope. Key management is one of the important security measure to secure communication in Vehicular Adhoc NETworks (VANETs) which assures that authorized vehicles and infrastructure components can communicate with each other only. To add an extra security layer to secure the unauthorized access and communication in the network, authors include intelligent key management into IDS.

Similarly, better deep learning and especially the advanced big data capable models represent another fruitful direction for future research. The more the data is produced from these VANETs, its real-time processing and analysis goes on increasing. The paper further argues that if the proposed IDS was extended to big data collected from real vehicular communication systems, it would be much more effective. However, if the IDS were able to train itself on volumes of real-world data this huge, it may increase its capacity at recognizing subtler and refined levels of attacks.

Additionally, the article discusses that popular machine-learning algorithm SVM: It can be done using advanced techniques like GA, ACO or PSO (Genetic Algorithms – Ant Colony Optimisation — Particle Swarm Optimization). Therefore, these optimization techniques may greatly improve the classification accuracy of SVM and as such make it more powerful to determine normal traffic from malicious ones in VANETs. The GA approach was the most effective of the three models at improving SVM performance. According to the authors they will attempt to elaboration AI-driven (deep learning, etc.) models for better optimization.

Furthermore, the paper discusses how safety messages are secured from any tampering attack by a malicious node (it is one of biggest treat in VANET security), as well. We propose an IDS that incorporates a new hybrid security model combining rule based filtering, event confident trust and historical knowledge to detect these attacks. It even makes use of the dempaster shafer theory as well as bayesian learning to solidify this process. Risk scoring is accomplished by combining evidence of an attack using the Dempster-Shafer theory, a mathematical means for modeling uncertainty. Short Memories: Again, anomalies in real-time can be classified by this model into the risk level of attacks without historical data whereas Bayesian learning updates it according to historical data and enhances them. Putting it all together like this will allow the IDS to get an accurate picture of how likely is that some sort of attack occurs and what can be done in order to defend us from it.

A number of experiments and comparative studies testify to the effectiveness of proposed IDS. The experiments demonstrate that the hybrid approach, originally proposed in this work by combining rule-

based filtering with Dempster-Shafer theory and Bayesian learning at pre-connection level greatly improves intrusion detection accuracy. In addition, the integration of multiple evidence sources and reasoning models enables to system to better characterize some more complex VANET patterns.

The article then suggests several ways in which future research and development can build upon this. A critical area of attention is the deployment of IDS in embedded hardware systems. This would allow testing under real-world traffic conditions as well as lessons learned on the system's performance and effectiveness in a live environment. Furthermore, the writers want to follow up with additional research focusing on scoring using a cyber threat questionnaire and user interviews. These studies will result in all addressable vulnerabilities or opportunities for the IDS as robust and effective as it can be.

The article ends with a thorough and futuristic method to make VANETs secure using an Intelligent IDS. The proposed IDS is very efficient detection of the cyber-attacks providing a level for securing networks utilizing machine-learning, deep learning and optimization algorithms. The future research directions described in the article imply that there still exist abundant opportunities for improving security of VANETs especially by exploiting big data, intelligent key management and embedded hardware implementations. Thereby, the need for resilient and adaptive security approaches like proposed IDS will make VANETs as a fundamental part of future Smart cities and ITS.

References:

[1] Alrawashdeh, K., Purdy, C.: Toward an online anomaly intrusion detection system based on deep learning. In: 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 195–200. IEEE (2016)
[2] Alsarhan, A., Al-Dubai, A.Y., Min, G., Zomaya, A.Y., Bsoul, M.: A new spectrum management scheme for road safety in smart cities. IEEE Transactions on Intelligent Transportation Systems 19(11), 3496–3506 (2018)
[3] Altwaijry, H.: Bayesian based intrusion detection system. In: IAENG Transactions on Engineering Technologies, pp. 29–44. Springer (2013)
[4] Bahrololum, M., Salahi, E., Khaleghi, M.: Anomaly intrusion detection design using hybrid of unsupervised and supervised neural network. International Journal of Computer Networks & Communications (IJCNC) 1(2), 26–33 (2009)
[5] Bhoi, S.K., Khilar, P.M.: Vehicular communication: a survey. IET networks 3(3), 204– 217 (2013)
[6] Bitam, S., Mellouk, A., Zeadally, S.: Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks. IEEE Wireless Communications 22(1), 96–102 (2015)
[7] Bu, S., Yu, F.R., Liu, X.P., Mason, P., Tang, H.: Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE transactions on vehicular technology 60(3), 1025–1036 (2010)
[8] Farid, D.M., Rahman, M.Z.: Attribute weighting with adaptive nbtree for reducing false positives in intrusion detection. arXiv preprint arXiv:1005.0919 (2010)
[9] Han, J., Kamber, M., Pei, J.: Data mining concepts and techniques third edition. Morgan Kaufmann (2011)
[10] Huang, Z., Ruj, S., Cavenaghi, M.A., Stojmenovic, M., Nayak, A.: A social network approach to trust management in vanets. Peer-to-Peer Networking and Applications 7(3), 229–242 (2014)
[11] Matura, Rishi & Singla, Kunal. (2024). Secure and User-Friendly Smart Home Automation: A Mobile-Centric IoT Approach. Journal of Trends in Computer Science and Smart Technology. 6. 10.36548/jtcsst.2024.2.007.
[12] Prathimesh, & Singla, Kunal & Shingari, Groresh & Sharma, Deepika. (2023). An Approach to Mine Data for Predicting Forest Fires Using Support Vector Machines and Gini Index for Feature Selection. 1457-1462. 10.1109/ICCPCT58313.2023.10245148.
[13] Sinha, Aditya & Singla, Kunal & Victor, Teresa Matoso. (2023). Artificial Intelligence and Machine Learning for Cybersecurity Applications and Challenges. 10.4018/978-1-6684-9317-5.ch007.

[14] Desale KS, Ade R (2015) Genetic algorithm based feature selection approach for effective intrusion detection system. In: 2015 International Conference on Computer Communication and Informatics (ICCCI), IEEE, pp 1–6
[15] Dhanabal L, Shantharajah S (2015) A study on nsl-kdd dataset for intrusion detection system based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering 4(6):446–452
[16] Eberhart R, Kennedy J (1995) A new optimizer using particle swarm theory. In: MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science, pp 39–43, DOI 10.1109/MHS.1995.494215
[17] Eberhart RC, Shi Y, Kennedy J (2001) Swarm intelligence. Elsevier Feng W, Zhang Q, Hu G, Huang JX (2014) Mining network data for intrusion detection through combining svms with ant colony networks. Future Generation Computer Systems 37:127–140
[18] Fouladi RF, Kayatas CE, Anarim E (2016) Frequency based ddos attack detection approach using naive bayes classification. In: 2016 39th International Conference on Telecommunications and Signal Processing (TSP), IEEE, pp 104–107
[19] G P, M J, M S (2018) An optimized decision tree approach for intrusion detection. Eurasian Journal of Analytical Chemistry 13(6):684–688
[20] Goldberg D (1989) Genetic algorithms in search, optimization, and machine learning, addison-wesley, reading, ma, 1989.
[21] NN Schraudolph and J 3(1) Goldberg DE (2006) Genetic algorithms. Pearson Education India Gupta N, Prasad R, Saurabh P, Verma B (2019) Nb tree based intrusion detection technique using rough set theory model. In: Data, Engineering and Applications, Springer, pp 93–101
[22] Hoi SCH, Rong Jin, Jianke Zhu, Lyu MR (2008) Semi-supervised svm batch mode active learning for image retrieval. In: 2008 IEEE Conference on Computer Vision and Pattern Recognition, pp 1–7, DOI 10.1109/CVPR.2008.4587350
[23] Holland JH, et al. (1992) Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. MIT press Hosseini S, Zade BMH (2020) New hybrid method for attack detection using combination of evolutionary algorithms, svm, and ann. Computer Networks p 107168
[24] Karaboga D (2005) An idea based on honey bee swarm for numerical optimization. Tech. rep., Technical report-tr06, Erciyes university, engineering faculty, computer . . .
[25] Li L, Yu Y, Bai S, Cheng J, Chen X (2018) Towards effective network intrusion detection: a hybrid model integrating gini index and gbdt with pso. Journal of Sensors 2018
[26] Ludwig SA (2017) Intrusion detection of multiple attack classes using a deep neural net ensemble. In: 2017 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, pp 1–7
[27] Dwivedi, Abhinav & Saini, Gurmeet & Ibrahim Musa, Usman & Singla, Kunal. (2023). Cybersecurity and Prevention in the Quantum Era. 1-6. 10.1109/INOCON57975.2023.10101186.
[28] Singla, Kunal & Singh, Baljap & Kaur, Er & Choudhary, Chahil. (2023). A Machine Learning Model for Content-Based Image Retrieval. 1-6. 10.1109/INOCON57975.2023.10101215.
[29] M. Yao, X. Wang, Q. Gan, Y. Lin, and C. Huang, "An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs," Security and Communication Networks, vol. 2021, Article ID 6698099, 12 pages, 2021.
[30] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 807–817, 2020.
[31] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-togrid communication," IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 6607–6618, 2019.
[32] N. B. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. Ur Rahman, "Efficient pairing-free Certificateless authentication scheme with batch verification for vehicular ad-hoc networks," IEEE Access, vol. 6, pp. 31808–31819, 2018.
[33] A. Nayyar, "Flying adhoc network (FANETs): simulation based performance comparison of routing protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP," in 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, August 2018.
[34] I. Naqvi, A. Chaudhary, and A. Rana, "Intrusion detection in VANETs," in 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, September 2021.

[35] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and countermeasures," Security and Communication Networks, vol. 2021, Article ID 9997771, 20 pages, 2021.

[36] A. Irshad, M. Usman, S. Ashraf Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," IEEE Transactions on Industry Applications, vol. 56, p. 1, 2020.

[37] S. M. Faisal and T. Zaidi, "Timestamp based detection of Sybil attack in VANET," International Journal of Network Security, vol. 22, no. 3, pp. 399–410, 2020.