MULTIMEDIA COMMUNICATIONS TECHNICAL COMMITTEE
http://www.comsoc.org/~mmc

MMTC Communications - Frontiers

Vol. 17, No. 1, January 2022

CONTENTS

SPECIAL ISSUE ON Security and Privacy of IoT and Mobile Networks

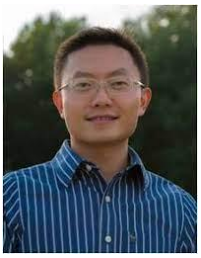
Guest Editor:[1] Lei Chen and [2] Narasimha Shashidhar
[1] Department of Information Technology, Georgia Southern University, GA, USA.
[2] Department of Computer Science, Sam Houston State University, TX, USA.
LChen@georgiasouthern.edu, Karpoor@shsu.edu

This special issue of IEEE MMTC Communications – Frontiers focuses on the advances in technologies and approaches to enhance the security and privacy of Internet of Things (IoT) and Mobile Networks. Four articles were selected for inclusion in this special issue. Three of these articles share their authors' innovative approaches utilizing deep learning methods for improved intrusion detection and object detection in vehicular networks, and the other paper focuses on protecting mobilecrowdsensing data and processing by using game theory and data encryption. These articles demonstrate the merit behind the integration of state-of-the-art artificial intelligence and machine learning algorithms to meet the increased demand for effective and efficient data security and privacy protection in IoT and mobile networks.

The first article sets its focus on improving the Controller Area Network (CAN) bus that manages the communication between electronic units in the automobile industry. Considering the strengths and limitations of the two popular artificial neural network solutions, the authors propose to bridge the use of Long Short-Term Memory (LSTM) and Bidirectional Gated Recurrent Unit (GRU) to identify and mitigate potential network intrusions in CAN bus systems. Experiments on KDD 99 and NSL-KDD show superior detection performance compared to existing methods.
The second research effort tackles the disentanglement in Domain-Invariant Object Detection (DAOD). In this research, the authors explore the potential behind utilizing Disentangled Representation Learning (DRL) by casting DRL into a process of vector decomposition and propose a novel disentangled method to extract Domain-Invariant Representations (DIR). The proposed methods were tested in both single-target and compound-target cases, where significant performance gain over the baseline demonstrates the effectiveness of the proposed disentangled method in both cases.

The third work focuses on enhancing the privacy protection mechanisms in Mobile Crowdsensing (MCS), where mobile data is collected and processed in extensive applications in the Industrial Internet of Things (IIoT). Based on game theory and data encryption schemes, the authors propose a personalized privacy protection framework where multiple security advancements are implemented. A personalized privacy measurement algorithm is proposed to calculate dynamic privacy levels, a rational upload strategy is designed based on privacy level, and a privacy-preserving data aggregation scheme is proposed. Theoretical and security analysis demonstrate a satisfactory balance between the quality of crowdsensing and user privacy offered by the proposed methods.

The authors of the fourth research article aim to evaluate and compare the resilience of Deep Reinforcement Learning (DRL) algorithms against cyberattacks. In Intelligent Transportation Systems (ITS), the Vision Zero initiative aims to eliminate all traffic-related fatalities and severe injuries. While autonomous vehicles play a critical role in achieving vision zero, the ITS data acquisition and processing systems are unfortunately prone to cyberattacks. This research thrust employs the CARLA driving simulations to investigate the resilience of Deep Q-learning (DQ) algorithms for autonomous driving. Various cyberattacks were tested, including DoS and replay attacks. Simulation results demonstrate that cyberattacks on LiDAR sensors have a minor impact on the DQN performance.



Dr. Lei Chen is an Associate Professor and Graduate Program Director with the Department of Information Technology at Georgia Southern University, GA, USA. He received his B.Eng. in Computer Science and Applications from Nanjing University of Technology, China, in 2000, and his Ph.D. in Computer Science and Software Engineering from Auburn University, USA, in August 2007. He joined Georgia Southern University in 2015, before when he served in the Department of Computer Science at Sam Houston State University, TX, USA, as the Graduate Program Coordinator for three master's programs and four graduate certificate programs. Dr. Chen is a Senior Member of the IEEE, and his research interests focus on the security, privacy and digital forensics of networks, information, cloud, Big Data, and mobile, handheld, and wireless networks. His scholarly activities were supported by the National Security Agency and the National Science Foundation. Dr. Chen has authored or co-authored over 100 scholarly works, including publications with high-impact journals and conferences. His edited and co-authored book Wireless Network Security: Theories and Practices, published by Springer in 2013, has received over 18,500 combined downloads. His edited/co-authored book Security, Privacy, and Digital Forensics in the Cloud, published by Wiley in 2019, was ranked top in the "21 Best New Digital Forensics Books to Read in 2019", and among the "98 Best Cloud Computing Books of All Time" and "100 Best Network Security Books of All Time" by Bookauthority.com. Dr. Chen has served as the editor, associate editor, and guest editor for multiple high-impact journals, such as the Elsevier Journal of Network and Applications and Springer MONET. He has been a regular reviewer for the IEEE IoT Journal, Elsevier Future Generation Computer Systems, and IEEE Transactions on Vehicular Technology, among others. He is also serving as chair and organizer for several international conferences and workshops.

Dr. Narasimha Shashidhar received his Bachelor of Engineering in Electronics and Communication Engineering from The University of Madras in 2001, and the M.S. and Ph.D. degrees in Computer Science and Engineering from The University of Connecticut in 2004 and 2010, respectively. He is currently an Associate Professor in the Department of Computer Science at Sam Houston State University, Huntsville, TX. His research interests include Cryptography, Information Hiding, Steganography, Electronic Voting and Security, Peer-to-Peer/Sensor Networks and Context-aware pervasive communication. He was a part of the Voting Technology and Research Center (VoTeR) at the University of Connecticut where he advised the State of CT on the security and deployment of electronic voting machines. He has over 50 conference/journal publications and serves in the editorial advisory/review board and the Technical Program Committee (TPC) of a number of books, journals and conferences. He is currently serving in the role of Director for the Doctor of Philosophy Program in Digital and Cyber Forensic Science. This is the first such doctoral program in the country and is designed to produce the future leaders in industry as well as academia in the field of digital forensics and cyber security.

LSTM and Bidirectional GRU based Intrusion Detection System for CAN bus Network

Asma Alfardus and Danda B. Rawat
Data Science and Cybersecurity Center
Howard University, Washington DC, USA
asma.alfardus@howard.edu, danda.rawat@howard.edu

Abstract
Since the advent of modern automobile industry, the complex distributed systems are being widely connected to external systems. Therefore, to manage the communications between these electronic units, the Controller Area Network (CAN) bus particularly serves as significant communique network. However, the potential rise in external systems and in-vehicle connections impose greater chances of security attacks in CAN network. Although CAN bus system is responsible for in-vehicle communications, it still lacks an effective mechanism for authentication and authorization. Furthermore, the messages of CAN bus system can broadcast easily in absence of basic security features, making the system more prone to network attacks. Therefore, a technique to protect modern vehicle memory (Long Short-Term Memory; LSTM) and Bidirectional Gated Recurrent Unit (GRU) as the main memory is needed to identify and mitigate the network intrusions in CAN bus system. Although LSTM technique is already used as system of intrusion detection to detect attacks in network of CAN bus, however, LSTM lacks defined mechanism for unknown attack detection making it less effective in systems more prone to unknown attacks. Therefore, we have combined the LSTM method with Bidirectional GRU to efficiently detect and mitigate the possible attacks in CAN bus network. Since GRU only uses hidden state to transfer the information and get rid of the cell state, we need to use the Bidirectional GRU which is more efficient and suitable for Intrusion detection system as a memory unit along with LSTM. Experiments on the well-known KDD 99 and NSL-KDD datasets show that the system has leading performance. The overall detection rate is 99.48% using KDD 99 and 99.39% using NSL-KDD with false positive rates as low as 0.04% and 0.71% respectively. Specifically, to detect attacks of denial of service (DOS), the system carried out detection charges of 99.989% on KDD 99 and 99.57% on NSL-KDD. Comparative experiments showed that LSTM+BGRU is more suitable as a memory unit for IDS. Moreover, bidirectional GRU can reach the high-quality overall performance in comparison with these days posted techniques.

1. Introduction

The automobile is probably the most essential shape of delivery of the contemporary age. It is said that the beginning of the modern vehicle dates returned, when a patent was filled for his invention by Karl Benz in 1886 which was known as the Benz patent motor-vehicle. The modern-day automobile has gone through many variations to emerge as more dependable, secure, and efficient. The controller location network (CAN) Bus protocol (Figure 1) is one of the most key adjustments added in the car enterprise. CAN is a dense communication bus of the International Organization for Standardization (ISO) responsible for the flow of Information between the digital manipulate devices (ECU) of an automobile. In simple terms, movement of the coordinates are created through the CAN bus protocol among the brakes, steering wheel, engine, etc. that is, it makes the modern-day automobile related. The CAN bus proto- col became at the start designed for industrial machines, instead it was taken on for the vehicle network communication. The modern vehicle consists of around 50 to one hundred ECUs, a number of which might be related by the CAN bus. Protocol of CAN bus be green for car network system due to its centralized and occasional-rate tool. CAN bus protocol is used to provide communication of ECU with messages. The ECU gets every message with distinctive CAN bus identifiers which might be used for internal interaction. Figure-1 shows the format of Can message in 11-bit mode. Many machines learning studies have developed technologies of intrusion detection with artificial intelligence. For ex- ample, Support vector machines (SVM), Artificial Neural networks (ANN) and Genetic algorithms (GA) have given excellent performance inside the discipline of intrusion detection. But the easy approach of machine learning suffers from many obstacles as the intrusion becomes an increasing number of complicated and diverse. Better getting to know strategies are wished, in automatic characteristic extraction and intrusion analysis. Although CAN bus system has lot of importance but despite that, the protocol of CAN bus is de- signed without protection functions, which makes it susceptible to availability, privacy and attacks of integrity. In vehicle communication structures, CAN bus protocol manage the messages which were send to the car system. A lot of sensor data speak to deliver messages to the CAN bus device. An ECU can percent manipulate records with an outside part of the auto through a network device. This closing possibility will increase the assault floor of the protocol of CAN bus system [1], [2]. The principal safety problems of the CAN bus system stand up as it transmits all ECU

messages without authentication or encryption [3]. Consequently, PC systems are unsafe to simple hacking strategies; consequently, assaulter can take control of the automobile's device easily and cause critical damage.

The Recurrent neural network (RNN) has didn't emerge as a main-stream net- work version within the beyond few years because of training and estimation difficulties. In latest years, with the evolution of deep learning concept, RNN has commenced to enter a period of fast improvement. Presently, RNN has already been correctly executed to speech recognition [4] and handwriting [5]. The number one characteristic of RNN is which circulates information in a hidden layer that could store formerly processed information, which has a structural advantage for processing time series information. Therefore, many intrusion behaviors can be abstracted as specific time series of underlying network events. Therefore, in this paper to improve the performance of detection and learning ability we have proposed an intrusion detection system which is based on LSTM and Bidirectional GRU followed by perceptron of multi-layer perceptron and module of SoftMax. The main goals of our article are given below

- To develop a datasets of CAN system attack (Spoofing, DoS, Fuzzing) using CAN messages from a real small vehicle or car.
- We are offering an efficient LSTM and Bidirectional GRU based intrusion detection system for on-board CAN bus network to recognize attacks by using the datasets KDD 99 and NSL-KDD.
- We have proposed an efficient preprocessing technique to make an efficient supervised classification model based on LSTM and Bidirectional GRU for the detection of CAN bus attacks.
- To make an Efficient CAN bus network Intrusion detection system (IDs) which are based on LSTM and Bidirectional GRU by selecting the best hyper-parameter values.

The rest of the paper is organized as follows. The Related work is described in section 2. Section 3 describe the Proposed methodology followed by the Experiments and Results in section 4.

2. Related Work

Koscher et al. demonstrate the injection of wireless communication attacks into vehicle network systems during a modern vehicle safety investigation. They used the Car-shark device to unmask numerous protection vulnerabilities at the CAN bus and tested that could transmission characteristics, whilst carried out to all nodes, facilitate an attacker's intrusion into messages from the network communication. Kl´eberger studied safety threats and attacks on car network structures, then mentioned special issues and their solutions. They also mentioned the intrusion detection system and the security capabilities of the architecture. Loukas et al. [5] suggested a deep learning of-based intrusion detection model for car network structures by using of multiple machine mastering structures binders. They executed their experiment by way of injecting cloud primarily based totally assaults on a robot car. Their outcomes display that the LSTM is quality appropriate for intrusion detection of vehicles with a standard accuracy of 86.89%. Spectral clustering (Sc) was adopted by Ma et al. [4] to take out functionality from network web site traffic and used a multi-layer Neural Network (DNN) to hit upon specific form of attacks with the quality rate accuracy. Although, the variables of weight and the thresholds of every DNN layer must be decided practically in preference to by means of careful mathematical concept. Kang [6] suggested an important DNN-based intrusion detection system for networks of vehicle. The system utilizes DNN to offer the threat to discriminate among normal packets and attack packets in a CAN bus network. To take benefit of deep learning, the device initializes the variables through preforming deep perception networks (DBNS), which improves accuracy of detection.

A hybrid model was suggested by Erfanii et al [7] which coupled a network of deep notion (DBN) with a one distinction of SVM. An unmonitored DBN was trained to take out preferred underlying functions, whilst an SVM of a category changed into educated from capabilities discovered out from db. This version supplied a green and accurate detection of anomaly approach appropriate for massive-scale and massive-scale domain names. A deep learning technique referred to as self-taught learning (STL) has been utilized by Javad et al. [8] to construct a system of intrusion detection network. Sparse car-encoders and NIDS primarily based on SoftMax regression had been implemented. Experiments performance of STL turned into the high-quality outcomes received in several previous studies. Ibrahim et al [9] used an unmonitored synthetic neural network to construct an intrusion detection machine primarily based on detection of anomaly. The system used ANN SOM (self-organizing map) for detection and to differentiate different attacks Site visitors from regular traffic. A classifier referred to as GPSVM based totally on genetic programming and SVM has been proposed by Pozi et al. [10] to enhance the detection fee of unusual attacks. Experimental end consequences proven that GPSVM can produce greater balanced category accuracy on the dataset of NSL-KDD without the want for re-sampling techniques or function selection. A method of hybrid combining genetic algorithm

(GA) and SVM has been suggested by Aslahii Shahrii et al [11]. The hybrid algorithm changed into used to lessen the wide variety of features from 45 to 10, and the set of rules of GA assigned those functions into 3 priorities. As a result, it showed very good values of actual positives and low false positives at the dataset of KDD-99. Hussain et al. [12] suggested a technique of step hybrid type. Within the first section, SVM became used for detection of anomaly, while inside the second segment, synthetic neural network became used for detection of abuse. The main concept changed into to mix the advantages of every approach to enhance the accuracy of the type. Simulation consequences primarily based on the NSL-KDD dataset established that this approach is going beyond the character classification of the ANN and SVM algorithms.

Shyu in 2003 proposed a new approach by using the usage of precept aspect analysis to discover anomalies or intrusions as outliers. Due to the fact outliers are very sensitive to outliers, facts set may be fashioned using random over- sampling or the artificial minority oversampling approach (smote) approach. This approach is ideal for the elegance of malicious phishing emails [13], [14]. Clustering is the manner of creating a statistics partition so that every institution consists of comparable characteristics. By finding an identical sample, the information can be separated. Due to the fact clustering can study from logging and manipulate the statistics itself, it has a large gain for intrusion detection [15]. The grouping of K-means mini lots produced very good precision to allocate several random groups of wonderful memory sizes, which enables the manner less difficult to bear in mind [16]. Because it requires unique batches, it takes a little time which prevents its use in exercise. Category schemes play a crucial function in detecting intrusions or anomalies for streaming information. To adapt a rapid network flow, Li et al. Proposed a k-nearest neighbor (KNN) classification in the implementation of wireless sensor networks [17], [18], [14]. Gadget learning algorithms which might be includes decision tree, rule-primarily based induction, Bayesian network, and genetic algorithm have dramatically progressed network safety. Currently, ensemble studying is used for classification strategies in the quest to keep away from false alarms. Ensemble precision classifier (aue) is a changed version of the accuracy weighted ensemble (awe) approach, which makes use of the concept of updating a classifier in step with the distribution [19]. Mohammed et al. [20] proposed a deep learning model for the network of fast learning based totally on particle swarm optimization (PSO) and implemented to the problem of intrusion detection. Methods of those deep learning to know strategies are effective and promising and can extract the specific problem features automatically without any prior strong knowledge. The recurrent neural network has shown great progress in this area however, Deep neural networks have a lot of parameters and non-linearity and still there are errors of detection such as unprecedented attacks low detection rate etc. So, in this paper we have proposed a novel technique which consist of LSTM and Bidirectional GRU for intrusion detection in CAN bus system and to improve the unknown attacks detection rate.

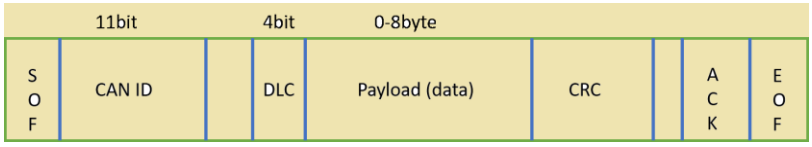


Figure 1: Format of CAN bus message in 11-bit mode with DLC of 8 where no safety features applied in this protocol.

3. Proposed Methodology

Recurrent Neural Network: There are different structures of RNNs including the simple and easiest structure suggested by Elman [21]. Within the machine of conventional neural net- work, that's go with the flow of information or records in one path, this is from the layer of input to hidden layer, and eventually on the layer of output. But the RNN is special: it could save the processed information at time 't' for the subsequent time calculation (t + 1; t + 2 ...). Consequently, the access of the hidden layer consists of no longer simplest the only exit of the top layer, but additionally the exist of same layer at the closing second. Conventional RNNs encounter leakage or explosion gradient problems [22]. To overcome these problems, specific structures of RNN are suggested. LSTM and BiGRU are two such type of models, and it makes use of some of gates to check memory and prevent the gradient from fading.

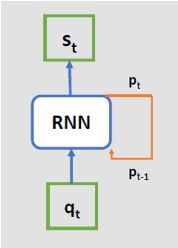


Figure 2: RNN basic architecture.

Long-Short-Term-Memory (LSTM)

LSTM is a special type of Recurrent neural networks. Schmidhuber and Hochreiter introduced it in 1997 [23]. We believe the LSTM is suitable along with bidirectional GRU for this research because the LSTM works well with regard to sequence classification and time series data. According to the architecture of the RNN (Fig. 2), one can proceed a data series *q1,…, qn* by using RNN and It will generate a series of outputs s1,. , si.

$$p_t = k_W(p_{t-1}, q_t) \tag{1}$$

where, p_t is new state, k_W is function along with parameter of weight 'W', p_{t-1} is old state and q_t is a input vector at step of time 't'. To get the new state p_t as an output, the same set of frameworks $k_W(p_{t-1}, q_t)$ are used in each step of time 't' with the old state of p_{t-1} and input q_t. The mathematical expression of recurrent sigma cell's are shown as:

$$p_t = \sigma(W_p p_{t-1} + W_q q_t + b) \tag{2}$$

$$s_t = p_t \tag{3}$$

where s_t is the cell output at time 't', p_t is the information of Recurrent, q_t is the input, the bias is 'b' and weights are W_p and W_q. Popular Recurrent cells in Recurrent networks are not able to cope with long-time period dependencies; as the gap between the related entries increases, it is tough to learn the relationship facts. Schmidhuber and Hochreiter proposed the LSTM cell in 1997 to control the problem of "prolonged-term addictions". They delivered the "door" into the mobile; for this reason, it enables the same old habitual cell to maintain reminiscence. Normally, the LSTM cellular indicates LSTM with a forgotten gate [24]. There are 3 ports in LSTM, and they may be chargeable for shielding and monitoring the nation of the cellular [25]. FIG. 3 illustrates the architecture of the LSTM cell made up of the load vector q_t, the hidden load vector p_{t-1} and the output vector p_t.

$$m_t = \sigma(W_m.[p_{t-1}, q_t] + b_m) \tag{4}$$

$$fg_t = \sigma(W_{fg}.[p_{t-1}, q_t] + b_{fg}) \tag{5}$$

$$D_t = \tanh(W_D.[p_{t-1}, q_t] + b_D) \tag{6}$$

$$E_t = fg_t * E_{t-1} + m_t * D_t \tag{7}$$

$$og_t = \sigma(W_{og}.[p_{t-1}, q_t] + b_{og}) \tag{8}$$

$$p_t = og_t * \tanh(E_t) \tag{9}$$

where, b_m, b_{fg}, b_D, b_{og} are the bias and W_m, W_{fg}, W_D, W_{og} are the weights, σ is called sigmoid function, 't' is current time of cell and 't-1' is the last or previous time of cell. The layer of sigmoid which is also called the layer of "forget gate" makes the decision and it gives the output between 0 and 1 value. The state of new cell is E_t which is got from the state of old cell E_{t-1} and is controlled by the input or load gate m_t and forget gate fg_t. The og_t is called output gate.

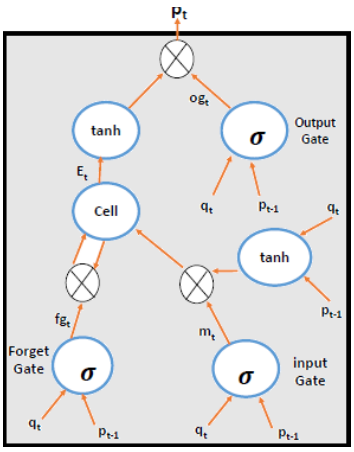


Figure 3: LSTM architecture.

Gated-Recurrent-Unit (GRU):

A GRU suggested in [26] is a new cell of memory which has been demonstrated to be powerful in different variations of packages (Figure 4). A GRU may be visible as a generalize form and is better version of LSTM and can be as compared in overall accomplishment to LSTM. In comparison to LSTM, GRU has fewer doors or gates. That is due to the fact the GRU has no mobile state and merge the enter and forgets ports right into a unmarried port, the replace port z. As a result, the GRU is a lot easier. In next experiments, GRU also confirmed a wonderful gain.

$$e_t = \sigma(W_e.[p_{t-1}, q_t] + q_t) \tag{10}$$

$$v_t = \sigma(W_v.[p_{t-1}, q_t]) \tag{11}$$

$$p'_t = \tanh(W.[v_t * p_{t-1}, q_t]) \tag{12}$$

$$p_t = (1 - e_t) * p_{t-1} + e_t * p'_t \tag{13}$$

$$\sigma = \frac{1}{1 + e^{-t}} \tag{14}$$

$$\tanh(t) = \frac{1 - e^{-2t}}{1 + e^{-2t}} \tag{15}$$

where, 'p' is the vector output, 'q' is the vector input, p' is the candidate output, 'W' is the weight parameter, 't' is the current time, 't-1' is the last or previous time, 'e' donates the reset gate, 'v' donates the update gate and tanh, σ are the activation or sigmoid functions which keeps the order of flowing information through GRU in a particular range.

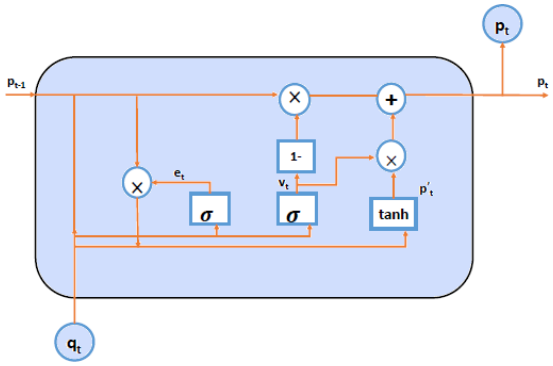


Figure 4: Architecture of GRU.

Regression of SoftMax

SoftMax regression is a generalize logistic regression which can gave a vector of N-Dimension σ(a) in the interval (0; 1) from a vector of N-dimension 'a' [27]

$$\sigma(a)_i = \frac{e^{ai}}{\sum_{n=1}^{N} e^{an}} \quad i = 1, ..., N \tag{16}$$

The network assaults of such type are distinctive, so any specific data have to be assigned to at least one in each of them (or every day). An IDS the use of a multi-classifier may be more suitable. A hypothesis feature is needed to make a multi-classifier, for a given input 'a' to estimate the chances for each (y=i-a) magnificence i. That is, we need to estimate the opportunity of each feasible type of output. In particular, the speculation characteristic must produce a vector of k-size (the sum of the elements of the vector is 1) to symbolize the envisioned opportunity

Multilayer-Perceptron

A multilayer perceptron is a type of unidirectional ANN made from many layers [28]. Using a nonlinear activation characteristic, MLP can discover indivisible linearly information. An MLP is characterized via sign of ahead propagation, mistakes of backward propagation, and is pushed with the aid of a Bp set of guidelines. The standard Bp set of regulations is a classical gaining knowledge of set of guidelines which calculates the difference a number of the actual output and the anticipated output, inverts the distinction at every degree, accordingly, adjusting the parameters of every degree to accumulate the gaining knowledge of goal. A normal MLP consists of 3 essential components: an input or input layer, more than one hidden layer, and a layer of output.

Overall Structure of IDS

To build a complete architecture, each component must be treated as a cascaded layer (Figure 5). The suggested intrusion detection system shape is demonstrated within the Figure 5. The machine includes a module of pre-processing, a LSTM and module of Bi-GRU, a module of MLP and a module of output. The module of pre-processing tactics the information to a strange value appropriate for the enter neural network without converting the dimensions of the information. The preprocessing set of rules for the experimental information set is proven below. The module of GRU includes one or greater GRU (bi-directional GRU) stages, used to extract and save features. It's far the coronary heart of the system. The module of MLP is model of n-layer perceptron, performing a nonlinear mapping from the output of the module of GRU which makes a nonlinear magnificence choice. Among the one's additives, the modules of LSTM, GRU and MLP are crucial for performance. Those modules are splendid kinds of neural networks. The LSTM and GRU has reminiscence, but it has a extra complicated shape. The mixture of the two bureaucracy deep networks which lets in to advantage a greater optimized result MLP has a smooth structure, speedy computation, and is straightforward to stack

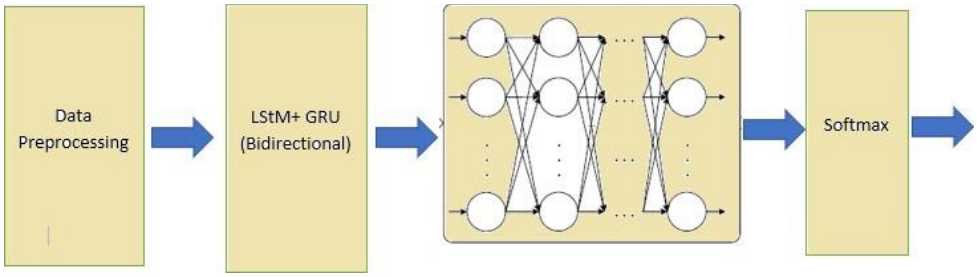


Figure 5: System Architecture.

4. Evaluation Experiments

Datasets

The great manner to assess an intrusion detection system is to apply a not un- usual dataset for trying out so that you can make a honest contrast of various structures. KDD 99 has been extensively used for decades within the assessment of SDIs and has grown to be the component general for benchmarking [29]. The dataset of KDD-99 was made totally on records obtained inside the Darpa'98 IDs experiment application MIT Lincoln labs. It holds 7 weeks of training records and 2 weeks of check statistics. This dataset consists of 39 assault types: 22 are in the schooling set and 17 appear handiest within the set as unknown assault types to check the generalization overall accomplishment of the set of regulations

A revised or new version of the KDD-99 dataset was proposed by Tavallaee et al. [31] which is named as NSL-KDD. The dataset of NSLKDD overcomes several shortcomings which were found in KDD 99. For example, it does now not encompass reproduction or redundant information. The variety of statistics decided on from every difficulty stage is extra suitable, which makes it extra efficient to get a truthful grade. The overall

wide form of statistics is cheap, permitting algorithms to be run at the finished dataset rather than a small, randomly decided on thing. As a end result, ratings from specific research can be in comparison very effortlessly. We've used these two datasets that are KDD-99 and NSL-KDD on this paper to assess the overall performance of proposed intrusion detection system.

Metrics: For the problems of classification, the classification results may be accurate or wrong, and all feasible consequences may be categorized steady with the following 4 conditions:

- True-Positive (Tp): classification of effective attacks.
- True-Negative (Tn): Classification of actual normal records.
- False Positives (Fp): Classification of real regular records which are known as attacks. This circumstance is likewise known as false alarms.
- False Negatives (Fn): Powerful attacks are categorized as regular recordings.

To simplify, Tp, Tn, Fp and Fn are the representation of four conditions numbers. Based on this, the detection rate, accuracy, precision, F-measure, and false positive rate can be defined as

$$Precision = \frac{Tp}{Tp + Fp} \tag{17}$$

$$Accuracy = \frac{tp + Tn}{Tp + tn + Fn + Fp} \tag{18}$$

$$False - positive - rate(Fpr) = \frac{Fp}{Fp + Tn} \tag{19}$$

$$DetectionRate(DR) = \frac{Tp}{Tp + Fn} \tag{20}$$

$$F - measure = \frac{2(Precision * DR)}{Precision + DR} \tag{21}$$

Precision is the range of accurate classifications out of the entire quantity of information. Precision is the quantity of powerful assaults proportional to the wide variety of categorized assaults. The detection rate (Dr) is the range categorized as assaults in percentage to the wide variety of actual attacks. The fake superb rate (FPR) is the wide variety labeled as assaults proportional to the quantity of all regular information.

Preprocessing of Data: The proposed system can best take delivery of virtual inputs, so you want to transform the non-digital facts in the dataset to digital facts. In each document, only 3 characteristics (Protocol kind, provider, and indicator) are transformed to numeric information. Encoding of '1' to 'n' is done to acquire this. Likewise, kind consequences are shown numerically ('1' to 'k1'), as given in Table 1.

Table 1: Classification of Coding-Identity

Identity classification	Code
DoS	01
R2R	02
U2R	03
Probee	04

Experimental Results

To objectively assess the model performance, experiments were executed 10 instances for cross validation at the KDD-99 and NSL-KDD datasets and the test tests used to evaluate performance. To decorate overall performance, cross entropy grows to be used as a feature rate instead of the least squares mistakes characteristic (Mse) [30]. The learning velocity and iterations form were set on at from realistic experience. The configuration of hyper parameter is given in Table 2. Within the suggested system, the modules of LSTM, Bi-GRU and MLP are very crucial. Hence, the experiments performance centered on checking these modules necessity and validity. Experiments have been completed on datasets of KDD-99 and NSL-KDD and results are given in Table 3 and Table 4. From those effects we finish that overall performance of our proposed approach LSTM+bi-GRU is higher than all different techniques on datasets of KDD-99 and NSL-KDD whose outcomes are referred to in desk three and four. It may be visible that the system the usage of LSTM+bi-GRU has benefits not simplest in phrases of accuracy, detection charge, however additionally with a fee of quicker convergence

Table 2: Hyper-Variable configuration.

Hyper-variable	value
Batch-size Epochs	64
Learning-rate	25
Momentum	0.001
Layers of MLP	0.8
Hidden nodes of MLP	3
Hidden units of RNN	48

Table 3: KDD 99 dataset experimental results.

Technique	Accuracy (%	DR(%)	FPR(%)
LSTM and BGRU	099.90	099.048	00.004
MLP and GRU	099.028	096.073	00.007
MLP and bLSTM	098.057	093.078	00.017
MLP and LSTM	098.051	094.077	00.053
GRU	092.028	071.077	00.013

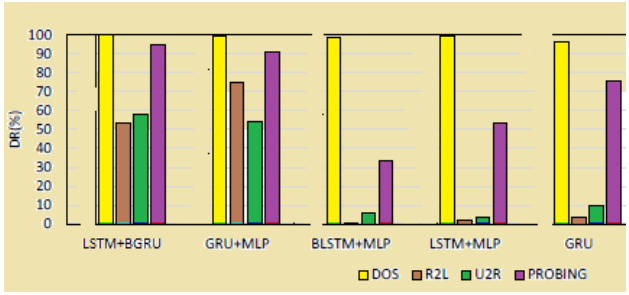
Table 4: NSL-KDD dataset experimental results.

Technique	Accuracy (%)	DR (%)	FPR (%)
LSTM and BGRU	99.030	99.039	00.071
MLP and GRU	99.019	96.035	01.000
MLP and bLSTM	96.041	95.065	02.067
MLP and LSTM	95.022	93.097	03.024
GRU	94.094	94.076	04.084

Discussion

To better the evaluation of the experimental effects, we have compared our proposed technique results with some other previous techniques as shown in Table 3 and 4 and in Fig. 6 and 7. From both tables 3 and 4, and Figures 6 and 7 we can see that LSTM + BGRU performed nicely on both datasets. By using KDD-99 and NSL-KDD datasets, we've got finished the top-notch accuracy, Dr and FPR. This contrast or assessment is a reference. Many IDs have different range in their responses of intrusion detection, and its miles hard to discover a tool that could acquire the first-rate normal overall accomplishment in every situation. Similarly, due to a moderate difference within the method of evaluation as an instance, datasets random sampling, the final consequences can also need to be one-of-a-type. Although, in comparison with modern research, we agree with that our proposed technique has great achievement in DR, Accuracy and FPR.

Figure 6: Results of detection rate on KDD-99.



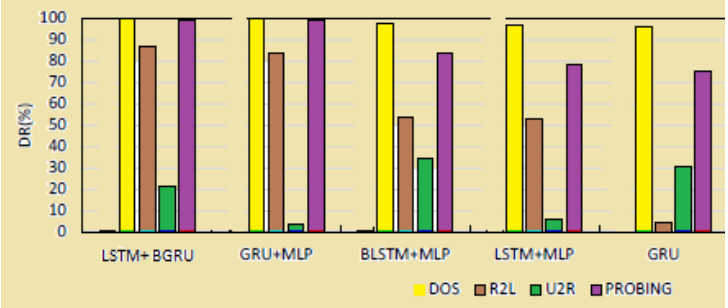


Figure 7: Results of detection rate on NSL-KDD.

The observation of u2r and r2l modified into no longer first-class. That is a not unusual hassle not in our proposed technique but also in other previous techniques. That is due to the motive that the recorded range of these two types of attacks have become too small. Such few data make extraction of the competencies with the useful resource of the gaining knowledge of set of rules useless, in order that the category accuracy isn't as high as for other measures. The probing and DoS assaults have extra obvious timing traits than u2r and r2l assaults, permitting a better detection normal overall performance to be carried out

5. Conclusion

In this article, we have proposed a new intrusion detection system. which uses LSTM and GRU as the primary repository unit, blended with MLP to emerge as privy to intrusions network. Techniques of deep learning have been used for the training and suitable performance changed into acquired. Experiments performed on the famous datasets of KDD-99 and NSL-KDD have demonstrated that our proposed model has high performance. The general rate of detection is is 099.48% on KDD-99 and 099.39% on NSL-KDD and with rate of false positive 00.04% and 00.71% respectively. In particular, DoS attack rate of detection is 099.99% on KDD-99 and 099.57% on NSL-KDD. Comparative results have been achieved on LSTM and GRU without or with bidirectional connections. The aggregate of LSTM, manner GRUs, and MLP has outperformed one of a kind presently published strategy. The system proposed on this report is specially based mostly on a theoretical verification. The next step may be to optimize the device or machine in order that it is able to be implemented to actual network environments and carried out greater effectively

References

[1] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in Proc. 16th Annu. Conf. Privacy, SECUr Trust (PST), Aug. 2018, pp. 16.

[2] M. L. Han, B. I. Kwak, and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," Veh. Commun., vol. 14, pp. 5263, Oct. 2018.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimen- tal sECUrity analysis of a modern automobile," in Proc. IEEE Symp.SECUr. Privacy, 2010, pp. 447462.

[4] T. Ma, F.Wang, J. Cheng, Y. Yu, and X. Chen, "A hybrid spectral clus- tering and deep neural network ensemble algorithm for intrusion detection in sensor networks," Sensors, vol. 16, no. 10, p. 1701, 2016.

[5] G. Loukas, T. Vuong, R. Hearteld, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," IEEE Access, vol. 6, pp. 34913508, 2018.

[6] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neu- ral network for in-vehicle network sECUrity," PloS one, vol. 11, no. 6, p. e0155781, 2016.

[7] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, "Highdi- mensional and large-scale anomaly detection using a linear one-class SVMwith deep learning," Pattern Recognition, vol. 58, pp. 121–134, 2016.

[8] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI In- ternational Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), New York, NY, USA, vol. 35, 2015, p. 2126.

[9] L. M. Ibrahim, D. T. Basheer, and M. S. Mahmod, "A comparison study for intrusion database (KDD99, NSL-KDD) based on self organization map (SOM) artificial neural network," Journal of Engineering Science and Technology, vol. 8, no. 1, pp. 107–119, 2013.

[10] M. S. M. Pozi, M. N. Sulaiman, N. Mustapha, and T. Perumal, "Improv- ing anomalous rare attack detection rate for intrusion detection system using support vector machine and genetic programming," Neural Process- ing Letters, vol. 44, no. 2, pp. 279–290, 2016.

[11] B. Aslahi-Shahri, R. Rahmani, M. Chizari, A. Maralani, M. Eslami, M. Golkar, and A. Ebrahimi, "A hybrid method consisting of GA and SVM for intrusion detection system," Neural Computing and Applications, vol. 27, no. 6, pp. 1669–1676, 2016.

[12] J. Hussain, S. Lalmuanawma, and L. Chhakchhuak, "A two-stage hy- brid classification technique for network intrusion detection system," In- ternational Journal of Computational Intelligence Systems, vol. 9, no. 5, pp.863–875, 2016.

[13] Ahsan, Mostofa, Rahul Gomes, and Anne Denton. "SMOTE Implemen- tation on Phishing Data to Enhance CybersECUrity." 2018 IEEE Interna- tional Conference on Electro/Information Technology (EIT). IEEE, 2018.

[14] Gomes, Rahul, Mostofa Ahsan, and Anne Denton. "Fusion of SMOTE and Outlier Detection Techniques for Land-Cover Classification Using Support Vector Machines."

[15] Seraphim, B. Ida, et al. "A Survey on Machine Learning Techniques in Network Intrusion Detection System." 2018 4th

International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.
[16] Peng, Kai, Victor CM Leung, and Qingjia Huang. "Clustering approach based on mini batch kmeans for intrusion detection system over big data." IEEE Access 6 (2018): 11897-11906.
[17] Li W, Yi P, Wu Y, et al. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network[J]. Journal of Electrical and Computer Engineering, 2014, 2014(5):1-8.
[18] Gomes, Rahul, Mostofa Ahsan, and Anne Denton. "Random Forest Clas- sifier in SDN Framework for User-based Indoor Localization." 2018 IEEE International Conference on Electro/Information Technology (EIT). IEEE, 2018.
[19] Ahmad, Iftikhar, et al. "Performance Comparison of Support Vector Ma- chine, Random Forest, and Extreme Learning Machine for Intrusion Dde- tection." IEEE Access 6 (2018): 33789-33795.
[20] M. H. Ali, B. A. D. Al Mohammed, A. Ismail, and M. F. Zolkipli, "A new intrusion detection system based on fast learning network and particle swarm optimization," IEEE Access, vol. 6, pp. 20 255–20 261, 2018.
[21] J. L. Elman, "Finding structure in time," Cognitive science, vol. 14, no. 2, pp. 179–211, 1990.
[22] J. Schmidhuber, "Deep learning in neural networks: An overview," Neural networks, vol. 61, pp. 85–117, 2015.
[23] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., vol. 8, no. 9, pp. 17351780, 1997.
[24] Y. Yu, X. Si, C. Hu, and J. Zhang, "A review of rECUrrent neural networks: LSTM cells and network architectures," Neural Comput., vol. 31, no. 7, pp. 12351270, Jul. 2019.
[25] Colah's Blog, Understanding LSTM Networks. Accessed: Aug. 15, 2020. [Online]. Available:https://colah.github.io/posts/2015-08-Understandig LSTMs/
[26] K. Cho, B. Van Merriënboer, D. Bahdanau, and Y. Bengio, "On the prop- erties of neural machine translation: Encoder-decoder approaches," Eighth Workshop on Syntax, Semantics and Structure in Statistical Translation, 2014.
[27] C. M. Bishop, "Pattern recognition," Machine Learning, vol. 128, pp. 1–58, 2006.
[28] S. K. Pal and S. Mitra, "Multilayer perceptron, fuzzy sets, and classifica- tion," IEEE Transactions on neural networks, vol. 3, no. 5, pp. 683–697, 1992.
[29] UCI, "KDD cup 1999 data," UCI, 1999. [Online]. Available: http://KDD.ics.uci.edu/databases/KDDcup99/[AccessedonDec.21,2016].
[30] J. Shore and R. Johnson, "Axiomatic derivation of the principle ofmaxi- mum entropy and the principle of minimum cross-entropy," IEEE Trans- actions on information theory, vol. 26, no. 1, pp. 26–37, 1980.
[31] M. Tavallaee, E. Bagheri,W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD cup 99 data set," in IEEE Symposium on Computational Intel- ligence for SECUrity and Defense Applications, 2009. CISDA 2009. IEEE, 2009, pp. 1–6

An Overview of Cooperative Perception in Autonomous Vehicles
Vector-Decomposed Disentanglement for Domain-Invariant Object Detection

Aming Wu[1], Rui Liu[1], Yahong Han[1], Linchao Zhu[2], Yi Yang[2]*
[1]Tianjin University, China, [2]University of Technology Sydney, Australia
tjwam@tju.edu.cn, ruiliu@tju.edu.cn, yahong@tju.edu.cn, Linchao.Zhu@uts.edu.au, yi.yang@uts.edu.au

1. Introduction

Though object detection has achieved many advances [27, 9, 42, 19, 26, 21], when the training and test data are from different domains, these methods usually suffer from poor generalization. To this end, the task of domain adaptive object detection (DAOD) [4] has been proposed, in which a domain gap always exists between the training/source and test/target domain, e.g., different weather conditions (as shown in Fig. 1).

(a) Daytime-sunny → Dusk-rainy

(b) Daytime-sunny → Night-rainy

Figure 1. To further verify the proposed method, we construct two new adaptive scenes with different weather conditions.

To address DAOD, many methods [31, 18, 35, 46] explored to reduce the domain gap by aligning the feature-level distribution of the source and single-target domain, which may neglect the impact of the domain-specific information existing in the aligned features. Towards DAOD, it is important to obtain domain-invariant representations (DIR), which is a bridge to alleviate the domain-shift impact and can help extract domain-invariant object features.

In this paper, we focus on extracting DIR. We explore to employ disentangled representation learning (DRL) [1, 24] to disentangle DIR from domain-specific representations (DSR). As a method of feature decomposition, the purpose of DRL is to uncover a set of independent factors that give rise to the current observation [6]. And these factors should contain all the information in the observation. Inspired by the idea, we explore to utilize DRL to solve DAOD and propose a novel disentangled method to extract DIR. Particularly, we cast DRL into a process of vector decomposition. Vector decomposition is the general process of breaking one vector into two or more vectors that add up to the original vector, which is similar in spirit to the process of disentanglement [13]. Thus, we consider employing the idea of vector decomposition to conduct disentanglement.

Concretely, given a feature map extracted by a backbone, an extractor consisting of multiple convolutional layers is devised to separate DIR from the feature map. Next, we take the difference between the feature map and DIR as DSR. Meanwhile, a domain classifier is used to help DSR contain much more domain-specific information. Besides, one key-step of disentanglement is to keep DIR and DSR independent. In this paper, we enhance independence via a constraint of vector orthogonalization between the DIR and DSR. Finally, a region proposal network (RPN) is utilized to extract object proposals from DIR. Moreover, since the proposed method is a new feature decomposition mechanism, we should design a proper optimization to obtain DIR. To this end, based on the purpose of DRL, we break DRL into two sequential training steps, i.e., the step of feature decomposition aiming at learning disentanglement, and the step of feature orthogonalization aiming at promoting DIR and DSR to be independent. The two-step optimization could promote our model learns feature decomposition, which is beneficial for extracting DIR for DAOD.

In the experiment, we first evaluate our method on the single-target case. Next, we evaluate our method on the compound-target case [23], i.e., the target is a compound of two different domains without domain labels.

The significant performance gain over baselines shows the effectiveness of our disentangled method. The main contributions of our work are as follows:

Contributions

Different from traditional disentanglement, we present a vector-decomposed disentanglement, which does not rely on the reconstruction operation to ensure the decomposed components contain all the information of input.

Based on vector-decomposed disentanglement, we design a new framework to solve DAOD. Meanwhile, we design a two-step training strategy to optimize our model.

In the experiment, our method is separately evaluated on the single- and compound-target cases. And we build two new adaptive scenes (see Fig. 1), i.e., Daytime-sunny→Dusk-rainy and Daytime-sunny → Night-rainy, to further verify our method. The significant performance gain over baselines shows the effectiveness of our method.

2. Related Work

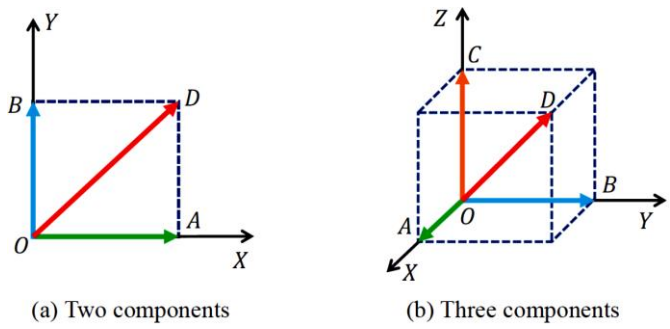
Most existing methods [39, 3, 40, 32, 44, 43] employ holistic representations to align the feature- or pixel-level distributions of the source and target domain. Particularly, Chen et al. [4] proposed to align the global feature distributions to reduce the domain gap. Saito et al. [29] proposed to align the local and global feature distributions to alleviate the domain-shift impact. Besides, the work [16] utilized an encoder-decoder network to translate the style of the source domain to that of the target domain, which could be thought of as aligning the pixel-level distributions of the source and target domain. Although these methods have been demonstrated to be effective, they neglect the impact of domain-specific information existing in the aligned features, which may affect the adaptation performance. To this end, we focus on extracting domain-invariant representations for DAOD.

As an effective mechanism of feature decomposition, recently, DRL [22, 2] has been demonstrated to be effective in many tasks, e.g., image translation [17] and few-shot learning [28]. Particularly, the work [17] employs DRL to decompose DSR to make diverse image style translation. Peng et al. [25] utilize DRL to disentangle three different factors to make domain adaptive classification. However, since this work only considers holistic image-level representations for classification, it could not be applied directly to object detection.

In this paper, we consider DRL from the perspective of vector decomposition. Particularly, our method only requires devising an extractor to decompose DIR. And DSR could be obtained from the difference between the input and DIR. Experimental results on single- and compound-target DAOD demonstrate the effectiveness of our method.

3. Vector-Decomposed Disentanglement

As discussed in the section of Introduction, the purpose of vector decomposition is to break one vector into two or more components that add up to the original vector. In general, each vector can be taken as the sum of two or more other vectors. Fig. 2 shows two decomposed examples, i.e., $\overrightarrow{OD} = \overrightarrow{OA} + \overrightarrow{OB}$ and $\overrightarrow{OD} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$.



(a) Two components (b) Three components

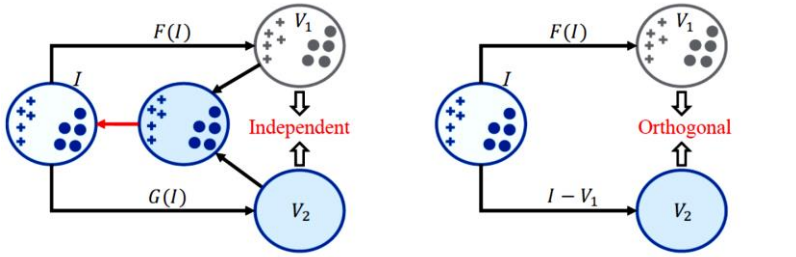
Figure 2. Two examples of vector decomposition.

Obviously, vector decomposition is similar in spirit to disentanglement. And the decomposition idea is also applied to high-dimensional space. Therefore, we consider employing vector decomposition to obtain disentangled representations. Concretely, for the case of two components (Fig. 3(b)), give an input representation I, we design an extractor F to decompose the first component V_1 from I. Then, we take the

difference between I and V_1 as the second component V_2. Here, we name the process extracting V_2 as difference decomposition.

$$V_1 = F(I), V_2 = I - V_1, V_1 \perp V_2, \quad (1)$$

where $\perp$ indicates two components are orthogonal.



(a) Traditional Disentanglement (b) Vector-Decomposed Disentanglement

Figure 3. Comparisons between the traditional method and our vector-decomposed method.

Compared with the traditional disentanglement (Fig. 3(a)), vector decomposition only takes the difference between the original input and decomposed components as the last component, which reduces parameters and computational costs. Moreover, the difference decomposition of obtaining the last component could make all the components contain all the information of the input, which does not rely on the reconstruction operation. In the following, we will introduce the details of vector-decomposed disentanglement for domain adaptive object detection.

4. Domain-Invariant Object Detection

For DAOD, we could access image x^s with labels y^s and bounding boxes b^s, which are from the source domain. And we could also access image x^t that is from the target domain. The goal is to obtain the results of the target domain.

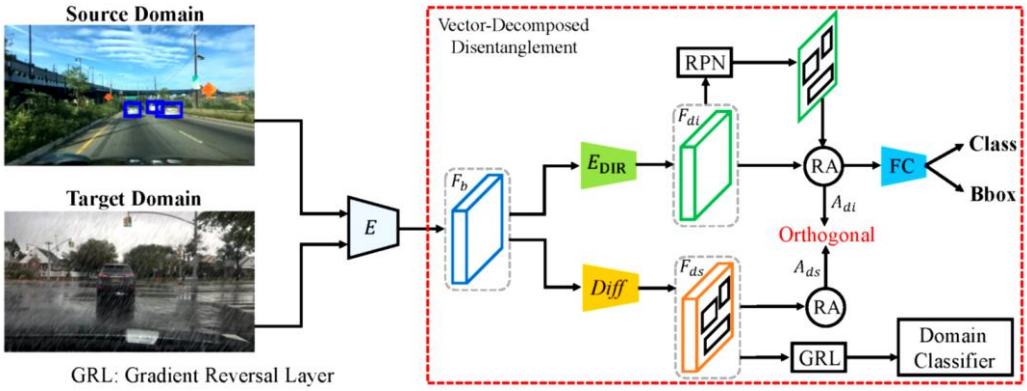


Figure 4. Illustration of vector-decomposed disentanglement.

The Network of Disentanglement

The right part of Fig. 4 illustrates the details of vector-decomposed disentanglement, which is plugged into the domain adaptive Faster R-CNN series [29, 39, 27]. Concretely, given an image x^s and x^t, we first obtain a feature map F_b that is the output of a feature extractor E. Next, we define an extractor E_{DIR} to decompose domain-invariant feature F_{di} from F_b. And the difference between F_b and F_{di} is taken as the domain-specific feature F_{ds}.

$$F_{di} = E_{DIR}(F_b), F_{ds} = F_b - F_{di}. \quad (2)$$

Here, E_{DIR} indicates the DIR extractor. The size of F_{di} and F_{ds} is set to the same as that of F_b. Next, a Region Proposal Network (RPN) is performed on F_{di} to extract a set of domain-invariant proposals. Finally, for an image from the source domain, the detection loss is defined as follows:

$$\mathcal{L}_{det} = \mathcal{L}_{loc} + \mathcal{L}_{cls} + \mathcal{L}_{rpn}, \quad (3)$$

where $\mathcal{L}_{loc}$ and $\mathcal{L}_{cls}$ separately indicate the bounding-box regression loss and classification loss. $\mathcal{L}_{rpn}$ is the loss of
RPN to distinguish foreground from background and to refine bounding-box anchors.

Training with the Two-step Optimization
The goal of our method (see Eq. (1)) is to decompose a set of orthogonal components. To enhance the disentangled ability, we break vector decomposition into two sequential steps. Specifically, we first promote models to be capable of decomposing components. Then, a constraint is imposed to promote these components to be orthogonal.

Figure 5. Illustration of our two-step optimization process. We only update the parameters in the blue blocks.

The step of feature decomposition. The step is to promote our model to decompose input features into two different components. Concretely, based on F_{di}, we first employ RPN to extract object proposals. Then, for a source image, the processes of detection loss are shown in Eq. (3).

Next, to promote the difference result F_{di} to contain much more domain-specific information, we utilize the adversarial training mechanism [8] and design a network C_{ds} to perform domain classification. And the domain label D is set to 0 for the source domain and 1 for the target domain. Finally, the loss of the first step is shown as follows:

$$\begin{cases} \mathcal{L}_{src}^{1} = \mathcal{L}_{det} + \mathcal{L}_{dom}\big(C_{ds}(F_{ds})\big), \\ \mathcal{L}_{tgt}^{1} = \mathcal{L}_{dom}\big(C_{ds}(F_{ds})\big), \end{cases} \tag{4}$$

where $\mathcal{L}_{src}^{1}$ and $\mathcal{L}_{tgt}^{1}$ are the objective functions of the source and target domain, respectively. $\mathcal{L}_{dom}$ is the domain
classification loss, i.e., $\mathcal{L}_{dom} = -\big[D\log\widehat{D} + (1-D)\log(1-\widehat{D})\big]$ and $\widehat{D} = C_{ds}(F_{ds})$. Finally, we take the sum of $\mathcal{L}_{src}^{1}$ and $\mathcal{L}_{tgt}^{1}$ to optimize the entire model.

The step of feature orthogonalization. In this step, we first fix the feature extractor E. Then, we use the extractor E_{DIR} to obtain F_{di} (Eq. (2)). Next, RPN is performed on F_{di} to extract a set of object proposals.

The key idea of disentanglement [6] is to keep the disentangled components independent. Here, based on the theory of vector decomposition, we try to promote the decomposed components are orthogonal, which is equivalent to the independent operation. Thus, we impose an orthogonal loss $\mathcal{L}_{\perp}$ on the DIR and DSR. Concretely, based on object proposals, we first obtain the Roi-Alignment result $A_{di} \in \mathbb{R}^{n\times c\times h\times w}$ of F_{di} and $A_{ds} \in \mathbb{R}^{n\times c\times h\times w}$ of F_{ds}, where n, c, h, and w indicate the number of proposals, the number of channels, the height and width, respectively. The process of orthogonal loss is shown as follows:

$$\begin{cases} M = (\|P_{di}\|_2^2) \odot (\|P_{di}\|_2^2), \\ \mathcal{L}_{\perp} = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n}\left|\sum_{j=1}^{c} M[i,j]\right|, \end{cases} \tag{5}$$

where $P_{di} \in \mathbb{R}^{n\times c}$ and $P_{ds} \in \mathbb{R}^{n\times c}$ are the results of global average pooling. $\|\cdot\|_2^2$, $|\cdot|$ and $\odot$ separately indicate L2-
norm, the absolute value operation, and element-wise product. $M[i,j]$ indicates the value of $M \in \mathbb{R}^{n\times c}$ at the position (i,j). Besides, it is worth noting that we use the alignment results instead of the overall feature map to compute the orthogonal loss, which could not only reduce computational costs but also promote our model to focus on object regions.

By minimizing the orthogonal loss, we could promote F_{di} and F_{ds} are independent. Since F_{ds} contains more domain-specific information, this loss can promote F_{di} to contain much more domain-invariant information. Finally, the loss of the second step is defined as follows:

$$\begin{cases} \mathcal{L}_{src}^2 = \mathcal{L}_{det} + \mathcal{L}_{dom}\big(C_{ds}(F_{ds})\big) + \mathcal{L}_{\perp}, \\ \mathcal{L}_{tgt}^2 = \mathcal{L}_{dom}\big(C_{ds}(F_{ds})\big) + \mathcal{L}_{\perp}, \end{cases} \tag{6}$$

where $\mathcal{L}_{det}$ is the detection loss based on A_{di}. The sum of $\mathcal{L}_{src}^2$ and $\mathcal{L}_{tgt}^2$ is used to optimize certain components of the model. The processes are shown in the right part of Fig. 5. After the second training step, the decomposed DIR and DSR will be kept independent, which enhances the disentangled ability of our model.

In this paper, our model is trained in an end-to-end way. The training details are shown in Algorithm 1. Besides, for the second training step, the parameters that do not appear in the step are fixed.

Algorithm 1 Two-step optimization for DAOD

Require:
source images $\{x^s, y^s, b^s\}$; target images $\{x^t\}$; feature extractor E; DIR extractor E_{DIR}; domain classifier C_{ds}.
Ensure:
feature extractor $\hat{E}$, DIR extractor $\hat{E}_{\mathrm{DIR}}$.
while not converged **do**
  Sample a mini-batch from $\{x^s, y^s, b^s\}$ and $\{x^t\}$;
  Feature Decomposition:
  Compute $\mathcal{L}_1 = \mathcal{L}_{src}^1 + \mathcal{L}_{tgt}^1$ (Eq. (4));
  Update E, E_{DIR}, and C_{ds} by $\mathcal{L}_1$;
  Update RPN module, Classifier, and Regressor by $\mathcal{L}_1$;
  Feature Orthogonalization:
  Compute $\mathcal{L}_2 = \mathcal{L}_{src}^2 + \mathcal{L}_{tgt}^2$ (Eq. (6));
  Update E_{DIR}, C_{ds} by $\mathcal{L}_2$;
  Update Classifier and Regressor by $\mathcal{L}_2$;
end while
return $\hat{E} = E$; $\hat{E}_{\mathrm{DIR}} = E_{\mathrm{DIR}}$.

Discussion about Learning DIR
For our method, we have two operations to promote to learn domain-invariant features. Firstly, the difference decomposition makes F_{di} contain much less domain-relevant information. Secondly, the orthogonal loss can further promote F_{di} to contain much more domain-irrelevant information. And we consider domain-irrelevant information contains domain-invariant information. Thus, these two operations promote F_{di} contains much more domain-invariant information, which reduces the domain-shift impact.

5. Experiment
In the experiment, we separately evaluate our approach on single- and compound-target DAOD. For the single-target case, our method is evaluated on four domain-shift scenes, i.e., Cityscapes [5]→FoggyCityscapes [30], PASCAL [7]→Watercolor [14], Daytime-sunny→Dusk-rainy, and Daytime-sunny→Night-rainy. For the compound-target case [23], we take Daytime-sunny as the source domain and the compound of Dusk-rainy and Night-rainy as the target domain, whose goal is to adapt a model from labeled source domain to unlabeled compound target domain. All the experiments are trained in an end-to-end way.

Datasets. Cityscapes is a dataset about city street scene. It contains 2,975 images for training and 500 images for validation. FoggyCityscapes is rendered based on Cityscapes. And it shows street scene under foggy weather. We follow the setting of the work [29] and evaluate our method on the validation set. For PASCAL→Watercolor, we utilize Pascal VOC dataset as the source domain. It contains 20 classes of images and bounding box annotations. Following the setting of the work [29], we employ Pascal VOC 2007 and 2012 training and validation splits for training, which results in about 15K images. Watercolor contains 2K images with 6 categories. The splits of the training and test set are the same as the work [29].

The Berkeley Deep Drive 100k (BDD-100k) dataset [41] consists of 100,000 driving videos. Based on this dataset, we build two new adaptive scenes. As shown in Fig. 1, for Daytime-sunny→Dusk-rainy, we select 27,708 daytime-sunny images as the source domain and 3,501 dusk-rainy images as the target domain. For Daytime-sunny→Night-rainy, we select 27,708 daytime-sunny images as the source domain and 2,494 night-

rainy images as the target domain. Besides, for the compound-target case, we select 27,708 daytime-sunny images as the source domain and 5,995 images consisting of dusk-rainy and night-rainy as the compound target domain. Meanwhile, we render these rainy images to enlarge the gap between the source and target domain. The number of annotation boxes is around 455,000. We evaluate the performance on the target domain. Besides, the BDD-100k dataset includes ten categories. Here, we choose seven commonly used categories, which do not include the category of light, sign, and train.

Implementation Details. We employ three convolutional layers as the domain-invariant feature extractor E_{DIR}. And we separately design a network with three fully connected layers as the domain classifiers. Finally, during training, we first train our model with learning rate 0.001 for 50K iterations, then with the learning rate 0.0001 for 30K more iterations. In the test, we utilize mean average precisions (mAP) as the evaluation metric.

Result Analysis of Single-target DAOD

Results on FoggyCityscapes. Table 1 shows the results of FoggyCityscapes. Here, VGG16 [33] is taken as the backbone. Through plugging our disentanglement into domain adaptive Faster R-CNN methods, the performance can be improved significantly. Particularly, for SW [29] and ICCR [39], our method separately improves the performance by 3.6% and 2.6%. This demonstrates decomposing domain-invariant features is helpful for alleviating the domain-shift impact on object detection.

Method	prsn	rider	car	truck	bus	train	mcycl	bcycl	mAP
Source Only	24.7	31.9	33.1	11.0	26.4	9.2	18.0	27.9	22.8
DAF [4]	25.0	31.0	40.5	22.1	35.3	20.2	20.0	27.1	27.6
DT [14]	25.4	39.3	42.4	24.9	40.4	23.1	25.9	30.4	31.5
SC-DA [45]	33.5	38.0	48.5	26.5	39.0	23.3	28.0	33.6	33.8
DMRL [16]	30.8	40.5	44.3	27.2	38.4	34.5	28.4	32.2	34.6
MLDA [38]	33.2	44.2	44.8	28.2	41.8	28.7	30.5	36.5	36.0
FSDA [36]	29.1	39.7	42.9	20.8	37.4	24.1	26.5	29.9	31.3
MAF [11]	28.2	39.5	43.9	23.8	39.9	33.3	29.2	33.9	34.0
CT [43]	32.7	44.4	50.1	21.7	45.6	25.4	30.1	36.8	35.9
CDN [34]	**35.8**	45.7	50.9	30.1	42.5	29.8	30.8	36.5	36.6
SCL [32]	31.6	44.0	44.8	30.4	41.8	40.7	33.6	36.2	37.9
ATF [12]	34.6	47.0	50.0	23.7	43.3	38.7	33.4	**38.8**	38.7
MCAR [44]	32.0	42.1	43.9	31.3	44.1	43.4	**37.4**	36.6	38.8
HTCN [3]	33.2	**47.5**	47.9	31.6	47.4	**40.9**	32.3	37.1	39.8
SW [29]	29.9	42.3	43.5	24.5	36.2	32.6	30.0	35.3	34.3
SW-VDD (ours)	32.1	42.8	49.4	29.0	49.0	33.9	29.9	37.1	37.9
ICCR [39]	32.9	43.8	49.2	27.2	45.1	36.4	30.3	34.6	37.4
ICCR-VDD (ours)	33.4	44.0	**51.7**	**33.9**	**52.0**	34.7	34.2	36.8	**40.0**

Table 1. Results (%) on adaptation from Cityscapes to FoggyCityscapes. 'prsn', 'mcycl', and 'bcycl' separately denote 'person', 'motorcycle', and 'bicycle' category. 'VDD' indicates vector-decomposed disentanglement.

The first row of Fig. 6 shows one detection example from the FoggyCityscapes dataset. Here, we take SW [29] as an example. We can see that compared with SW, our method localizes and recognizes objects existing in the foggy image accurately. This further shows our method is effective.

(a) Raw image (b) GT (c) SW baseline (d) One Step Training (e) Two-Step Training

Figure 6. Detection results on the FoggyCityscapes and Watercolor scene.

Results on Watercolor. Table 2 shows the Watercolor results. Here, we use ResNet101 [10] as the backbone. We can see plugging vector-decomposed disentanglement into SW [29] improves its performance significantly. Besides, MCAR [44] exploits multi-label object recognition as a dual auxiliary task to improve

the alignment. We can see that our method outperforms MCAR by 0.6%. These all demonstrate our method is effective. And our method could alleviate the impact of the watercolor style.

The second row of Fig. 6 shows one watercolor example. We can see compared with SW, our method could localize and recognize objects accurately. These further demonstrate employing vector-decomposed disentanglement could indeed alleviate the domain-shift impact.

Method	bike	bird	car	cat	dog	person	mAP
Source Only	68.8	46.8	37.2	32.7	21.3	60.7	44.6
BDC-Faster [29]	68.6	48.3	47.2	26.5	21.7	60.5	45.5
DAF [4]	75.2	40.6	48.0	31.5	20.6	60.0	46.0
WST-BSR [15]	75.6	45.8	49.3	34.1	30.3	64.1	49.9
MAF [11]	73.4	55.7	46.4	36.8	28.9	60.8	50.3
DC [20]	76.7	53.2	45.3	**41.6**	35.5	**70.0**	53.7
ATF [12]	78.8	**59.9**	47.9	41.0	34.8	66.9	54.9
SCL [32]	82.2	55.1	**51.8**	39.6	38.4	64.0	55.2
MCAR [44]	87.9	52.1	**51.8**	**41.6**	33.8	68.8	56.0
SW [29]	82.3	55.9	46.5	32.7	35.5	66.7	53.3
SW-VDD (ours)	**90.0**	56.6	49.2	39.5	**38.8**	65.3	**56.6**

Table 2. Results (%) on adaptation from Pascal to Watercolor.

Results on Dusk-rainy. Table 3 shows the results of Daytime-sunny→Dusk-rainy. ResNet101 [10] is taken as the backbone. We can see that for this scene, the adaptation performance of state-of-the-art methods, e.g., CT [43] and HTCN [3], is weak. Besides, we can also see that plugging the disentanglement into SW [29] and ICCR [39] improves their performance significantly. The performance is separately improved by 5.4% and 2.9%. This further demonstrates vector-decomposed disentanglement is capable of disentangling domain-invariant features, which is helpful for alleviating the domain-shift impact on object detection.

Method	bus	bike	car	motor	person	rider	truck	mAP
Source Only	38.6	21.5	51.7	12.0	19.7	13.6	40.9	28.3
CT [43]	35.5	20.3	50.9	7.9	21.6	16.1	34.4	26.7
SCL [32]	34.8	19.2	50.8	13.2	25.9	18.0	38.1	28.6
HTCN [3]	35.9	21.1	51.1	13.7	24.0	16.6	39.0	28.8
DAF [4]	43.6	27.5	52.3	16.1	28.5	21.7	44.8	33.5
SW [29]	40.0	22.8	51.4	15.4	26.3	20.3	44.2	31.5
SW-VDD	46.1	31.1	54.4	25.3	**31.0**	22.4	47.6	36.9
ICCR [39]	43.8	28.5	52.4	22.7	29.2	21.9	45.6	34.9
ICCR-VDD	**47.9**	**33.2**	**55.1**	**26.1**	30.5	**23.8**	**48.1**	**37.8**

Table 3. Results (%) on adaptation from Daytime-sunny to Dusk-rainy.

The first row of Fig. 7 shows three detection examples of the dusk-rainy scene. We can see that this is a challenging adaptation scene. The images are very obscure. Our method localizes and recognizes objects existing in these images accurately, which further demonstrates the effectiveness of vector-decomposed disentanglement.

Figure 7. The first and second row separately show the detection results on the “Daytime-sunny→Dusk-rainy” and “Daytime-sunny→Night-rainy”.

Results on Night-rainy. Table 4 shows the results of Daytime-sunny→Night-rainy. ResNet101 [10] is taken as the backbone. We can see that for this scene, the performance of many adaptation methods [3, 32, 43] is

weak. For example, the mAP value of HTCN and CT is lower than 20%. Plugging the disentanglement into SW [29] and ICCR [39] improves their performance significantly. The performance is improved by 5.7% and 3.1%. Particularly, for each object category, our method outperforms SW [29] and ICCR [39]. This further demonstrates the effectiveness of vector-decomposed disentanglement.

Method	bus	bike	car	motor	person	rider	truck	mAP
Source Only	23.4	13.3	31.8	1.5	10.2	10.9	23.2	16.3
CT [43]	22.4	9.7	27.4	0.6	9.3	9.3	13.4	13.1
SCL [32]	20.0	9.2	33.2	0.3	11.9	10.6	26.4	15.9
HTCN [3]	22.8	9.4	30.7	0.7	11.9	4.8	22.0	14.6
DAF [4]	23.8	12.0	37.7	0.2	14.9	4.0	29.0	17.4
SW [29]	24.7	10.0	33.7	0.6	13.5	10.4	29.1	17.4
SW-VDD	31.7	15.3	38.0	**11.1**	18.2	16.7	**30.8**	23.1
ICCR [39]	32.5	12.1	36.2	1.3	16.1	17.0	29.3	20.6
ICCR-VDD	**34.8**	**15.6**	**38.6**	10.5	**18.7**	**17.3**	30.6	**23.7**

Table 4. Results (%) on Daytime-sunny→Night-rainy.

The second row of Fig. 7 shows three detection examples of the night-rainy scene. We can see for this scene, the brightness of images is very low. Meanwhile, the rainy images are very obscure. Our method localizes and recognizes objects existing in the night-rainy images accurately. This demonstrates extracting domain-invariant representations is helpful for alleviating the domain-shift impact. Our method could extract domain-invariant representations effectively.

Ablation Analysis

Based on the single-target case, we plug our method into SW [29] to make an ablation analysis. Table 5 shows the results. We can see that for our model, employing two training steps is effective. Particularly, two-step training outperforms one-step training by 3.4% and 2.1%. This shows our optimization mechanism promotes the model to extract domain-invariant representations, which is beneficial for DAOD. In Fig. 6(d), we show two examples based on one training step. We can see using two training steps could detect objects existing in the two images accurately. Moreover, we can also see that the orthogonal loss could improve the performance significantly. This shows the orthogonal loss is indeed helpful for promoting DIR and DSR to be independent, which improves the disentangled ability.

Method	One-step	Two-step	OL	C → F	V → W
SW-VDD	✓			33.2%	52.7%
SW-VDD	✓		✓	34.5%	54.5%
SW-VDD		✓		36.5%	54.9%
SW-VDD		✓	✓	**37.9%**	**56.6%**

Table 5. Ablation analysis of our method.

Compared with traditional disentanglement. To further demonstrate the effectiveness of our method, we replace our method with the traditional disentanglement [25, 37]. Other components are kept unchanged. We employ the same training steps to optimize the model. Based on FoggyCityscapes and Watercolor dataset, the adaptation performance of the traditional disentanglement is 34.1% and 54.6%, which is weaker than our method. Besides, since our method does not include the reconstruction stage, our method owns much fewer parameters and computational costs. These all demonstrate the performance of our method outperforms the traditional disentangled method. Meanwhile, this also shows that our vector-decomposed disentanglement could extract domain-invariant features effectively, which improves the detection performance.

Visualization analysis. In Fig. 8, we compare DIR extracted by our disentangled method and traditional disentanglement. We find that compared with traditional disentanglement, the DIR extracted by our vector-decomposed disentanglement contains much less domain-specific information. Particularly, for these examples, we can see that the DIR extracted by the traditional disentanglement contains much more domain-specific information, e.g., the TD-DIR (Fig. 8(f)) of the bird image, which leads to the incorrect detections. This further demonstrates the effectiveness of our vector-decomposed disentanglement.

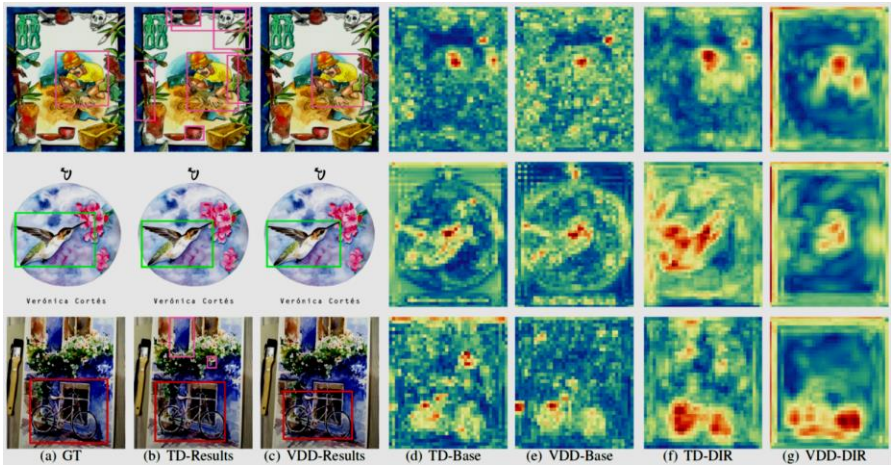


Figure 8. Comparisons of feature maps extracted by our vector-decomposed disentanglement (VDD) and traditional disentanglement (TD).

Result Analysis of Compound-target DAOD

For compound-target DAOD, we use the same optimization method as that of the single-target case. ResNet101 is the backbone. Table 6, 7, and 8 show the compared results. Here, the model trained on the compound-target DAOD is separately evaluated on the compound target, dusk-rainy, and night-rainy domain. Compared with SW [29], plugging our disentanglement into SW improves its performance by 5.3%, 5.6%, and 5.0%. Meanwhile, we can see that the performance of each category outperforms all compared methods significantly. This shows for single- and compound-target DAOD, extracting DIR is an efficient way. Meanwhile, the performance gain further demonstrates our method is capable of extracting DIR effectively.

Method	bus	bike	car	motor	person	rider	truck	mAP
Source Only	35.1	19.3	44.0	8.8	17.5	12.8	37.7	25.0
DAF [4]	35.9	18.3	44.2	10.1	22.0	17.9	39.9	26.9
CT [43]	31.3	15.4	41.7	8.4	19.1	15.3	32.3	23.4
SCL [32]	32.7	19.7	44.9	10.5	22.9	18.5	38.3	26.8
SW [29]	36.9	20.7	45.1	6.6	23.1	16.9	41.5	27.3
ICCR [39]	38.8	20.4	44.6	11.7	24.7	15.4	41.6	28.2
SW-VDD	**41.8**	**26.8**	**48.6**	**17.9**	**27.0**	**22.2**	**44.1**	**32.6**

Table 6. Results (%) on the compound target domain.

Method	bus	bike	car	motor	person	rider	truck	mAP
Source Only	38.6	21.5	51.7	12.0	19.7	13.6	40.9	28.3
DAF [4]	39.5	21.0	51.6	12.6	24.8	20.5	42.7	30.4
CT [43]	34.9	17.6	49.8	11.6	21.9	17.9	35.6	27.0
SCL [32]	35.7	22.3	50.7	14.8	25.3	19.9	40.1	29.8
SW [29]	39.2	24.6	49.6	9.2	25.5	19.3	43.7	30.1
ICCR [39]	42.0	21.9	51.5	16.5	27.2	16.8	44.1	31.4
SW-VDD	**43.7**	**30.3**	**52.7**	**22.3**	**29.7**	**24.8**	**46.4**	**35.7**

Table 7. Results (%) on the dusk-rainy scene.

Method	bus	bike	car	motor	person	rider	truck	mAP
Source Only	23.4	13.3	31.8	1.5	10.2	10.9	23.2	16.3
DAF [4]	24.2	11.0	32.4	4.6	12.7	11.9	27.7	17.8
CT [43]	19.5	9.7	29.0	1.1	9.9	9.1	17.6	13.7
SCL [32]	22.9	12.8	35.8	0.9	14.8	15.0	30.2	18.9
SW [29]	29.6	10.4	37.9	0.7	15.0	11.1	31.6	19.5
ICCR [39]	28.4	16.5	33.6	0.9	16.4	12.2	30.3	19.7
SW-VDD	**35.7**	**17.4**	**42.2**	**7.9**	**18.1**	**16.0**	**33.9**	**24.5**

Table 8. Results (%) on the night-rainy scene.

6. Conclusion

In this paper, we propose vector-decomposed disentanglement for DAOD. We only define an extractor to extract domain-invariant representations. Meanwhile, we do not use reconstruction to ensure the disentangled components contain all the information in the input. In the experiment, our method is separately

evaluated on the single- and compound-target case. The performance gain over baselines shows the effectiveness of our method.

References

[1] Yoshua Bengio, Aaron Courville, and Pascal Vincent. Representation learning: A review and new perspectives. IEEE transactions on pattern analysis and machine intelligence, 35(8):1798–1828, 2013.

[2] Ruichu Cai, Zijian Li, Pengfei Wei, Jie Qiao, Kun Zhang, and Zhifeng Hao. Learning disentangled semantic representation for domain adaptation. In Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, pages 2060–2066, 2019.

[3] Chaoqi Chen, Zebiao Zheng, Xinghao Ding, Yue Huang, and Qi Dou. Harmonizing transferability and discriminability for adapting object detectors. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 8869–8878, 2020.

[4] Yuhua Chen, Wen Li, Christos Sakaridis, Dengxin Dai, and Luc Van Gool. Domain adaptive faster r-cnn for object detection in the wild. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 3339–3348, 2018.

[5] Marius Cordts, Mohamed Omran, Sebastian Ramos, Timo Rehfeld, Markus Enzweiler, Rodrigo Benenson, Uwe Franke, Stefan Roth, and Bernt Schiele. The cityscapes dataset for semantic urban scene understanding. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 3213–3223, 2016.

[6] Kien Do and Truyen Tran. Theory and evaluation metrics for learning disentangled representations. arXiv preprint arXiv:1908.09961, 2019.

[7] Mark Everingham, Luc Van Gool, Christopher KI Williams, JohnWinn, and Andrew Zisserman. The pascal visual object classes (voc) challenge. International journal of computer vision, 88(2):303–338, 2010.

[8] Yaroslav Ganin and Victor Lempitsky. Unsupervised domain adaptation by backpropagation. arXiv preprint arXiv:1409.7495, 2014.

[9] Kaiming He, Georgia Gkioxari, Piotr Doll´ar, and Ross Girshick. Mask r-cnn. In Proceedings of the IEEE international conference on computer vision, pages 2961–2969, 2017.

[10] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 770–778, 2016.

[11] Zhenwei He and Lei Zhang. Multi-adversarial fasterrcnn for unrestricted object detection. arXiv preprint arXiv:1907.10343, 2019.

[12] Zhenwei He and Lei Zhang. Domain adaptive object detection via asymmetric tri-way faster-rcnn. European Conference on Computer Vision, 2020.

[13] Irina Higgins, David Amos, David Pfau, Sebastien Racaniere, Loic Matthey, Danilo Rezende, and Alexander Lerchner. Towards a definition of disentangled representations. arXiv preprint arXiv:1812.02230, 2018.

[14] Naoto Inoue, Ryosuke Furuta, Toshihiko Yamasaki, and Kiyoharu Aizawa. Cross-domain weakly-supervised object detection through progressive domain adaptation. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 5001–5009, 2018.

[15] Seunghyeon Kim, Jaehoon Choi, Taekyung Kim, and Changick Kim. Self-training and adversarial background regularization for unsupervised domain adaptive one-stage object detection. In Proceedings of the IEEE/CVF International Conference on Computer Vision, pages 6092–6101, 2019.

[16] Taekyung Kim, Minki Jeong, Seunghyeon Kim, Seokeon Choi, and Changick Kim. Diversify and match: A domain adaptive representation learning paradigm for object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 12456–12465, 2019.

[17] Hsin-Ying Lee, Hung-Yu Tseng, Jia-Bin Huang, Maneesh Singh, and Ming-Hsuan Yang. Diverse image-to-image translation via disentangled representations. In Proceedings of the European Conference on Computer Vision (ECCV), pages 35–51, 2018.

[18] Shuang Li, Chi Harold Liu, Xie Binhui, Limin Su, Zhengming Ding, and Gao Huang. Joint adversarial domain adaptation. In Proceedings of the 27th ACM International Conference on Multimedia, pages 729–737, 2019.

[19] Xin Li, Fan Yang, Hong Cheng, Junyu Chen, Yuxiao Guo, and Leiting Chen. Multi-scale cascade network for salient object detection. In Proceedings of the 25th ACM International Conference on Multimedia, page 439447, 2017.

[20] Feng Liu, Xiaoxong Zhang, Fang Wan, Xiangyang Ji, and Qixiang Ye. Domain contrast for domain adaptive object detection. arXiv preprint arXiv:2006.14863, 2020.

[21] Wei Liu, Dragomir Anguelov, Dumitru Erhan, Christian Szegedy, Scott Reed, Cheng-Yang Fu, and Alexander C Berg. Ssd: Single shot multibox detector. In European conference on computer vision, pages 21–37. Springer, 2016.

[22] Yen-Cheng Liu, Yu-Ying Yeh, Tzu-Chien Fu, Sheng-De Wang, Wei-Chen Chiu, and Yu-Chiang Frank Wang. Detach and adapt: Learning cross-domain disentangled deep representation. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 8867–8876, 2018.

[23] Ziwei Liu, Zhongqi Miao, Xingang Pan, Xiaohang Zhan, Dahua Lin, Stella X Yu, and Boqing Gong. Open compound domain adaptation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 12406–12415, 2020.

[24] Francesco Locatello, Stefan Bauer, Mario Lucic, Sylvain Gelly, Bernhard Sch¨olkopf, and Olivier Bachem. Challenging common assumptions in the unsupervised learning of disentangled representations. 2019.

[25] Xingchao Peng, Zijun Huang, Ximeng Sun, and Kate Saenko. Domain agnostic learning with disentangled representations. ICML, 2019.

[26] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi. You only look once: Unified, real-time object detection. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 779–788, 2016.

[27] Shaoqing Ren, Kaiming He, Ross Girshick, and Jian Sun. Faster r-cnn: Towards real-time object detection with region proposal networks. In Advances in neural information processing systems, pages 91–99, 2015.

[28] Karl Ridgeway and Michael C Mozer. Learning deep disentangled embeddings with the f-statistic loss. In Advances in Neural Information Processing Systems, pages 185–194, 2018.

[29] Kuniaki Saito, Yoshitaka Ushiku, Tatsuya Harada, and Kate Saenko. Strong-weak distribution alignment for adaptive object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 6956– 6965, 2019.

[30] Christos Sakaridis, Dengxin Dai, and Luc Van Gool. Semantic foggy scene understanding with synthetic data. International Journal of Computer Vision, 126(9):973–992, 2018.

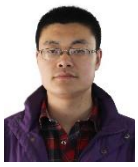
[31] Rui Shao, Xiangyuan Lan, and Pong C Yuen. Feature constrained by pixel: Hierarchical adversarial deep domain adaptation. In Proceedings of the 26th ACM international conference on Multimedia, pages 220–228, 2018.

[32] Zhiqiang Shen, Harsh Maheshwari, Weichen Yao, and Marios Savvides. Scl: Towards accurate domain adaptive object detection via gradient detach based stacked complementary losses. arXiv preprint arXiv:1911.02559, 2019.

[33] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556, 2014.

[34] Peng Su, Kun Wang, Xingyu Zeng, Shixiang Tang, Dapeng Chen, Di Qiu, and Xiaogang Wang. Adapting object detectors with conditional domain normalization. European Conference on Computer Vision, 2020.
[35] Jindong Wang, Wenjie Feng, Yiqiang Chen, Han Yu, Meiyu Huang, and Philip S Yu. Visual domain adaptation with manifold embedded distribution alignment. In Proceedings of the 26th ACM international conference on Multimedia, pages 402–410, 2018.
[36] TaoWang, Xiaopeng Zhang, Li Yuan, and Jiashi Feng. Few-shot adaptive faster r-cnn. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 7173–7182, 2019.
[37] Aming Wu, Yahong Han, Linchao Zhu, and Yi Yang. Instance-invariant domain adaptive object detection via progressive disentanglement. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021. doi: 10.1109/TPAMI.2021.3060446.
[38] Rongchang Xie, Fei Yu, Jiachao Wang, Yizhou Wang, and Li Zhang. Multi-level domain adaptive learning for cross-domain detection. arXiv preprint arXiv:1907.11484, 2019.
[39] Chang-Dong Xu, Xing-Ran Zhao, Xin Jin, and Xiu-Shen Wei. Exploring categorical regularization for domain adaptive object detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 11724–11733, 2020.
[40] Minghao Xu, Hang Wang, Bingbing Ni, Qi Tian, and Wenjun Zhang. Cross-domain detection via graph-induced prototype alignment. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 12355–12364, 2020.
[41] Fisher Yu,Wenqi Xian, Yingying Chen, Fangchen Liu, Mike Liao, Vashisht Madhavan, and Trevor Darrell. Bdd100k: A diverse driving video database with scalable annotation tooling. arXiv preprint arXiv:1805.04687, 2018.
[42] Jiahui Yu, Yuning Jiang, ZhangyangWang, Zhimin Cao, and Thomas Huang. Unitbox: An advanced object detection network. In Proceedings of the 24th ACM international conference on Multimedia, pages 516–520, 2016.
[43] Ganlong Zhao, Guanbin Li, Ruijia Xu, and Liang Lin. Collaborative training between region proposal localization and classification for domain adaptive object detection. In European Conference on Computer Vision, pages 86–102. Springer, 2020.
[44] Zhen Zhao, Yuhong Guo, Haifeng Shen, and Jieping Ye. Adaptive object detection with dual multi-label prediction. In European Conference on Computer Vision, pages 54–69. Springer, 2020.
[45] Xinge Zhu, Jiangmiao Pang, Ceyuan Yang, Jianping Shi, and Dahua Lin. Adapting object detectors via selective cross-domain alignment. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 687–696, 2019.
[46] Junbao Zhuo, Shuhui Wang, Weigang Zhang, and Qingming Huang. Deep unsupervised convolutional domain adaptation. In Proceedings of the 25th ACM international conference on Multimedia, pages 261–269, 2017.

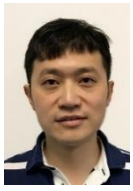
Aming Wu received the Ph.D. degree from Tianjin University, Tianjin, China, in 2021. He joins Xidian University as a pre-tenured associate professor at the School of Electronic Engineering in Jan. 2021. His current research interests include computer vision, multimedia analysis, and machine learning.



Rui Liu received the B.S. degree from Northeastern University, Shenyang, China, in 2019. He is currently pursuing the M.S. degree with the College of Intelligence and Computing, Tianjin University, Tianjin, China. His research interests include computer vision and object detection.

Yahong Han received the Ph.D. degree from Zhejiang University, Hangzhou, China, in 2012. He is currently a full professor with the College of Intelligence and Computing, Tianjin University, Tianjin, China. From Nov. 2014 to Nov. 2015, he visited Prof. Bin Yu's group at UC Berkeley as a Visiting Scholar. His current research interests include multimedia analysis, computer vision, and machine learning.

Linchao Zhu received the Ph.D. degree in computer science from University of Technology Sydney, Australia, in 2019. He received the B.E. degree from Zhejiang University, China, in 2015. He is currently a lecturer in the Australian Artificial Intelligence Institute, University of Technology Sydney, Australia. His research interests are video analysis and understanding.



Yi Yang received the Ph.D. degree in computer science from Zhejiang University, Hangzhou, China, in 2010. He is currently a professor with the University of Technology Sydney, Australia. He was a post-doctoral researcher in the School of Computer Science, Carnegie Mellon University, Pittsburgh, Pennsylvania. His current research interests include machine learning and its applications to multimedia content analysis and computer vision, such as multimedia indexing and retrieval, surveillance video analysis, and video content understanding.

A Personalized Privacy Protection Framework for Mobile Crowdsensing in IIoT

Rong Ma, Lanzhou University of Technology, China
Jinbo Xiong, Fujian Normal University, China*
MiaRonGer@163.com, jbxiong@fjnu.edu.cn

1. Introduction

With the rapid digitalization of various industries, mobile crowdsensing (MCS), an intelligent data collection and processing paradigm of the Industrial Internet of Things (IIoT), has provided a promising opportunity to construct powerful industrial systems and provide industrial services. The existing unified privacy strategy for all sensing data results in excessive or insufficient protection and low quality of crowdsensing services (QoCS) in MCS. To tackle this issue, we propose a personalized privacy protection (PERIO) framework [1] based on game theory and data encryption.

The main contributions of the PERIO framework are fourfold:

- According to the sensing user's historical spatio-temporal trajectory information, a personalized privacy measurement algorithm is proposed to calculate dynamic privacy levels by using the metrics of public attributes and personalized attributes.
- A rational uploading strategy is designed based on the privacy level and an incomplete information game, while the Nash equilibrium is obtained to make a reasonable balance between high QoCS and personalized privacy.
- Based on additively homomorphic encryption, a privacy-preserving data aggregation scheme is proposed to effectively protect confidentiality, integrity and real-timeness of the uploaded data.
- Theoretical and security analysis show that the strategy is rational, and the aggregation scheme is provably secure. Ample simulation results with real trajectory dataset indicate that PERIO provides a satisfactory balance between the QoCS and user's privacy, and guides sensing users to choose the optimal strategy to maximize user utility.

The rest of this paper is organized as follows: related works and problem formulation are presented in Section II and Section III. In section IV, we elaborately describe the PERIO framework. Section V analyzes the PERIO framework in the aspects of security and performance. Section VI summarizes the entire paper.

2. Related Work

The existing research on data privacy protection of MCS can be divided into four categories: anonymity, differential privacy, encryption, and game theory.

In the study of anonymity, Agir et al. [2] proposed a user-adaptive location privacy protection scheme. By setting a personal privacy threshold and combining user-denied privacy protection levels, multiple noises adding spatial cloaking units are generated to achieve privacy protection and flexibility. The scheme can resist against background knowledge attacks, but it lacks effective privacy level metrics and is computationally expensive. In the study of differential privacy, Huo et al. [3] proposed a real- time streaming data aggregation framework with adaptive event differential privacy for the privacy protection of real-time data aggregation and distribution. Despite its advantage of privacy protection, the original Laplacian noise used in the proposed methods is unbounded, which affects the data utility. In the study of encryption methods, Agir et al. [2] proposed a novel user-side location privacy-protection scheme that adopts an adaptive strategy for adjusting the privacy threshold to meet personalized location-privacy protection requirements. The proposed scheme balances the personal location-privacy concerns and the sensing data utility. However, these schemes are not suitable for mobile users in MCS because computationally expensive and communication overloading by requiring multiple rounds of interaction operations in the online phase. In addition, there are game theory methods to protect data privacy in MCS, Xiong et al. [4] proposed a novel secure multiparty auction mechanism based on the auction game theory to effectively address the prisoner's dilemma problem. However, these schemes focus on data privacy protection based on game theory but lack the consideration of individual private information of users.

3. Problem Formulation

This section describes the system model and security requirements of the PERIO framework. Introduced the connotation of QoS, followed by problem description.

3.1 System Model

We consider the system model of the PERIO framework under a typical MCS architecture, including a semi-trusted sensing platform, a large number of sensing users, and multiple cloud service providers (CSP) involved in final data transactions, as shown in Fig .1.

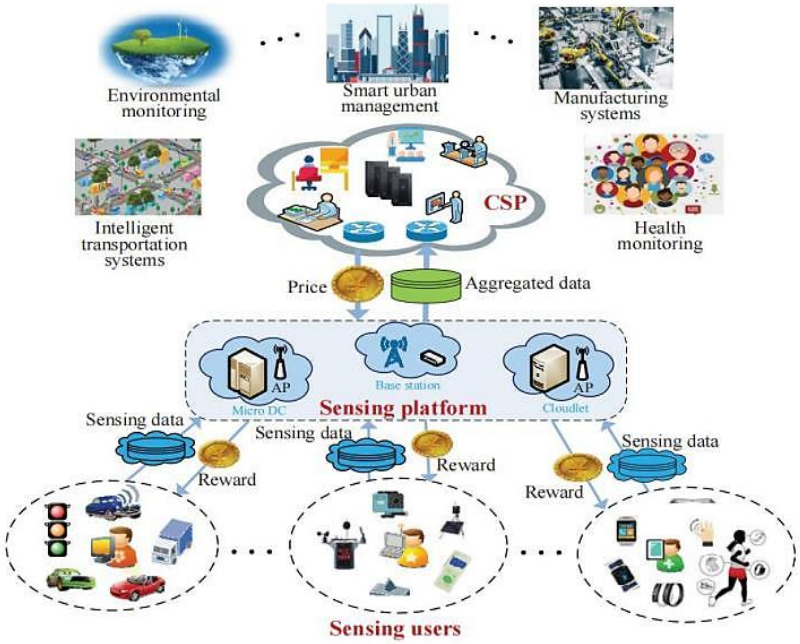


Fig. 1. System model of the PERIO framework

- According to the different privacy requirements, each sensing user chooses to participate in the spatio-temporal sensing task and uploads the spatio-temporal sensing data. In exchange, the user will receive corresponding rewards from CSP via sensing platform.
- CSP is responsible for purchasing data through the platform and providing follow-up services to the requester with different privacy requirements. Rational CSPs strive to acquire high QoCS data from platform at a reasonable price.
- The platform calculates real-time personalized privacy level for each user, issues tasks and interacts with users and CSP. Meanwhile, it sells the collected data to CSP and returns its rewards to the user using an appropriate strategy. The platform can be implemented by employing fog nodes or edge nodes.

3.2 Problem Description

In an intelligent transportation service in the IIoT, a user chooses strategy to upload the data of both the road and the autonomous vehicle to the platform, and the CSP then estimates the current road condition according to the uploaded information and provides real-time regional road condition information and navigation services for requesters. The QoCS, in terms of real-time road condition provided by the CSP, depends on the number of users who upload their data. It is assumed that the user set is willing to upload their data in order to obtain a greater *Qi* value. Due to the fact that different users may have different privacy levels at different locations, the users are then bound to bring a certain privacy loss. The objective is to find an uploading scheme that maximizes the total privacy levels and satisfies $Q \geq Q_{min}$. The following two factors must be considered in this intelligent transportation service: ①measuring user i's LP_i at a certain location l_j; ②i may not know the privacy requirements of other users.

To solve the first issue, we consider the metrics of the natural attributes of a location l_j and personalized attributes of i at that location. For the second issue, we employ an incomplete information game, assigning a user type at a certain location, where user type meets the probability distribution and indicates the privacy of i at that location.

4. Construction of the PERIO Framework

In this section, we elaborately present the following three components to construct the PERIO framework: personalized privacy measurement, rational uploading strategy, and privacy-preserving data aggregation scheme.

4.1 Personalized Privacy Measurement

Public attributes refer to the unified functional status of the location for all users. Locations with different public attributes may have various private information to different users, who may have different privacy levels. For example, the public attributes of a hospital, bank, park, supermarket, field, and river can be very different. For patients, a hospital has a high privacy level, and patients' health status and medical information cannot be exposed to unauthorized parties. However, people have less privacy concerns at places such as supermarkets, parks, wilderness, or rivers as they contain less or no private information that would jeopardize users' personal interests. Therefore, the public attributes of the location can be preliminarily determined according to its GPS information.

Personalized attributes refer to the private attributes of a specific user at a certain location, which may vary from person to person in terms of their social relations. Personalized attributes consist of access duration, access frequency and access regularity.

- Access duration. According to the historical trajectory record of a user over a period of time, the average access time of the user at each location can then be obtained, which reflects the degree of dependency of the user to the locations.
- Access frequency, which refers to the ratio of the user's access to a certain location to the total access frequency of all the locations over a period of time in MCS.
- Access regularity. In order to reflect users' regular access to a certain location and measure the variance of separation cycles.

4.2 Rational Uploading Strategy

To achieve a balance between privacy protection and QoCS, we present a user uploading behavior game (UBG) by adopting incomplete information game theory in MCS and analyze Bayesian Nash equilibrium of UBG to construct a rational uploading strategy to protect user privacy.

UBG. User set represents a current user set at a given location. Based on incomplete information game, the reward function privacy level of the pre-game participants, and user determines its strategy function.

Bayesian Nash Equilibrium. The balance of UBG games can be obtained by comparing the average rewards of uploading and non-uploading and calculating the balance threshold of user uploading according to the strategy used.

Strategy Description. We propose a rational data uploading strategy based on the UBG game, which provides not only the QoCS Q but also effective privacy LP for achieving the overall optimization. The proposed strategy is a user-centered mechanism as they can decide whether to upload data according to their personalized privacy requirements.

4.3 Privacy-preserving Data Aggregation Scheme

In an MCS system, data leakage always occurs, and privacy is compromised when users upload data to the platforms. In order to tackle this issue, this section describes our privacy- preserving data aggregation scheme based on the idea of additively homomorphic encryption (AHE) [5], which effectively protects data confidentiality, integrity and ensures real-timeness. The implementation consists of four phases.

System initialization phase. Some users broadcast their ID and cluster request to all their neighbor nodes. After receiving this message, the user sends feedback to join the cluster. This process continues until the entire network is divided into multiple clusters. Each user has a different key shared with the platform. Disclosing any single user key would not allow an attacker to access other users' data. During the key distribution process, the network broadcasts each key generated by RC4 to the corresponding user nodes. Each user node generates and initializes a counter for the platform to verify whether each user uploads the latest data to ensure the real-time data and resist replay attacks.

Data preparation stage. After receiving the task request from the platform, each user collects data m to participate in the task according to the proposed reasonable upload strategy, and the user encrypts the data C using the AHE algorithm idea, which ensures the data privacy during the upload process. After encrypting the data, each user calculates the corresponding $H(m)$ to help the platform verify data integrity. Each cluster node uploads the message $(C, H(m))$ to its cluster head node.

Data aggregation stage. The cluster head node aggregates the ciphertext uploaded by each user to reduce the amount of data uploaded. At the same time, the cluster head node aggregates the received verification codes into a Unicode and uploads the aggregated data. That is, the cluster head node uploads $(C_{AGG}, H(_{AGG}))$ to the platform.

Data verification stage. After receiving the aggregated data from the head node, the platform decrypts the ciphertext. After the ciphertext is received from the platform, the homomorphic hash verification code $H'(_{AGG})$ can be computed for integrity checking by comparing it with the $H(_{AGG})$ received from the platform. When these two codes are equal, it can be concluded that the data has not been tampered with or forged during the upload process, and the platform accepts the received data. Otherwise, the received data will be discarded.

5. Analysis and Evaluation

In this section, a comprehensive analysis of the proposed privacy-preserving data aggregation scheme is presented in terms of system security analysis, computational cost and communication overhead.

5.1 Security analysis

Table I compares the AHE scheme [5], the efficient secure aggregation (ESA) scheme [6], and our scheme in terms of achieved security goals. Our scheme effectively ensures that the data can securely reach the platform without leakage during the transmission process. In addition, our scheme enables the platform to verify the integrity of the received data thereby avoiding any tampering of private data in the uploading process. Finally, to prevent replay attacks, the platform can verify the real-timeness of the received private data.

Security Metrics	AHE [5]	ESA [6]	Our Scheme
Confidentiality	Yes	Yes	Yes
Integrity	No	Yes	Yes
Real-timeness	No	No	Yes

Table 1. Security Comparison of Different Schemes

Schemes	Computational Cost	Communication Overhead
AHE [5]	$C_M + C_A$	$2{:}45 \times 10^4$B
ESA [6]	$C_M + C_A + 2C_{hash}$	$4{:}1 \times 10^4$B
Our scheme	$C_M + C_A + C_{hash}$	$2{:}65 \times 10^4$B

Table 2. Comparison of Computation and Communication

5.2 Computational cost and communication overhead

Table II shows the comparison of the computational costs and communication overhead among the three aggregated encryption schemes. Our scheme has a slightly higher computational cost than that of AHE for the reason that for the purpose of integrity protection each user node computes the message authentication code of its data in our scheme. Table III also indicates that the communication overhead of our scheme is slightly greater than that of AHE. This is because AHE only requires the upload of private data during the upload process, where the platform is however incapable of judging whether the received data has been tampered with.

5.3 Performance Evaluation

The simulation is implemented in C++ and runs on a Windows 7 platform with Intel Xeon E5-2650 v3@2.30GHz processor and 8GB memory. Real data set collected from the GeoLife project [47] is used in this simulation. The data points in the data set are collected by GPS recorders with different acquisition frequencies at intervals of 2-5 seconds. The acquisition time lasted from April 2007 through August 2012. The data set contains 18670 GPS track records of 182users, including 24.87 million data points, which can serve as a typical spatio-temporal sensing data set. The proposed strategy is compared with the Adaptive scheme [2] based on the adaptive privacy protection strategy and static privacy protection scheme (SPPS) [7] under the same simulation environment.

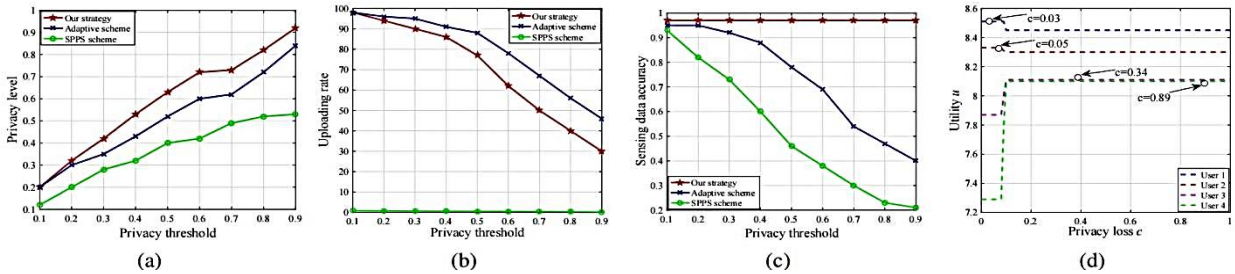


Fig. 2. Experiment analysis of our framework compared with related works: (a) Comparison of privacy protection levels; (b) Comparison of data uploading rate; (c) Comparison of data accuracy; (d) Incentive compatibility of our strategy

Privacy protection level. The location privacy leakage probability is used to measure the privacy protection level of different schemes. The comparative simulation results are shown in Fig.2(a). The privacy protection levels of all three schemes are on the rise with the increase of privacy threshold and thereby implementing the

privacy protection of participants' location. Our strategy has a higher privacy protection level than the Adaptive scheme, which suffers from occasional privacy leakage even after location confusion treatment despite its dynamic measuring participants' privacy level. In our strategy, sensing users dynamically choose whether to participate in data sensing tasks at a location according to the privacy of the location, thereby satisfying different users' privacy requirements.

Data uploading rate. The data uploading rate is measured by the ratio between the amount of uploaded data to the total amount of data. The comparative simulation results are shown in Fig.2(b). The data uploading rate of all three schemes decreases when privacy threshold increases as the higher the privacy threshold, the more the data to hide to achieve a higher privacy protection level. In our strategy, users whose privacy is lower than or equal to the privacy threshold at a certain location would upload data, while others would not, thereby effectively avoiding the problem of data loss.

Data accuracy. Data accuracy is measured by the mean absolute error of data. The comparative simulation results are shown in Fig.2(c). With the increase of privacy threshold, the data accuracy of SPPS [30] and Adaptive [26] decreases gradually, while the data accuracy of our strategy remains at 98%. Under the premise of meeting participants' privacy requirements, participants in our strategy tend to submit accurate data. In terms of data accuracy, our strategy has noticeable advantages in sensing scenarios requiring high spatial-temporal correlation.

Incentive compatibility. This section examines the incentive compatibility of our strategy. Four users were randomly selected for personalized privacy metrics and privacy loss calculations and were allowed to report different false privacy losses compared to their final utility value for reporting real privacy losses. The marks in Fig.2(d) are the utility values corresponding to the users' real privacy losses. When the user chooses to report true privacy loss, the utility value is the greatest and the incentive compatibility is satisfied. The utility value will not increase when users choose to report false privacy losses.

6. Conclusion

In this paper, we proposed the PERIO framework for MCS services in IIoT, which consists of a personalized privacy measurement algorithm, a rational uploading strategy, and a privacy-preserving data aggregation scheme. This framework satisfies the requirements of QoCS, improves the privacy level, and maximizes users' utility. Theoretical analysis and ample simulation results using real trajectory dataset demonstrate the comprehensive advantages of the PERIO framework over the existing schemes in typical scenarios.

References

[1] J. Xiong, R. Ma, L. Chen, et al., A personalized privacy protection framework for mobile crowdsensing in IIoT, IEEE Transactions on Industrial Informatics, 2020, 16(6):4231-4241, DOI:10.1109/TII.2019.2948068.
[2] B. Agir, T. Papaioannou, R. Narendula, et al., User-side adaptive protection of location privacy in participatory sensing, Geoinformatica, 2014, 18(1): 165-191.
[3] Y. Huo, C. Yong, Y. Lu, Re-adp: Real-time data aggregation with adaptive-event differential privacy for fog computing, Wireless Communications and Mobile Computing, 2018, Article ID 6285719, 2018:1-13.
[4] J. Xiong, R. Ma, L. Chen et al., Achieving incentive, security, and scalable privacy protection in mobile crowdsensing services, Wireless Communications and Mobile Computing, 2018, 2018:1-10.
[5] C. Castelluccia, E. Mykletun, G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks, in Proceedings of the MOBIQUITOUS, 2005, 109-117.
[6] L. Hu, D. Evans, Secure aggregation for wireless networks, in Proceedings of the IEEE SAINT, 2003, 384-391.
[7] J. Krumm, A survey of computational location privacy, Personal and Ubiquitous Computing, 2009, 13(6):391-399.

Evaluation of Deep Reinforcement Learning Algorithms for Resiliency against Cyberattacks

Godwyll Aikins[1], Sagar Jagtap[1],Weinan Gao[1,], Di Zhang[2], and Timo T. Hämäläinen[2]*
[1] Florida Institute of Technology, Melbourne, FL USA 32901
[2] University of Jyväskylä, Jyväskylä, Finland 40014
** Corresponding Author: wgao@fit.edu*

1. Introduction

The development of internet of things (IoT) devices and sensing, analysis, control, and communication technologies has advanced the realization of intelligent transportation systems (ITS) and contributed toward vision zero, an initiative to eliminate all traffic-related deaths and severe injuries. In ITSs, autonomous vehicles (AVs) play a critical role in achieving vision zero. An AV needs to process a vast number of ITS data acquired via a variety of sensors and communication channels to function autonomously. However, because of their dependency on communications and data processing, they are highly vulnerable to cyberattacks. The consistency and dependability of such information are vital for AV safety and security. Deep reinforcement learning (DRL) algorithms are touted as a security solution addressing intra-vehicle attacks as they can account for the interconnection of cyber and physical layers of AVs. Although DRL solutions have the potential to increase the driving performance of AVs, their resilience to cyberattacks has yet to be fully investigated. This paper aims to evaluate the resilience of DRL algorithms to cyberattacks.

1.1. Reinforcement Learning

Reinforcement learning (RL), a branch of machine learning (ML), aims to teach an agent to learn independently by interacting with its surroundings [1]. Unlike supervised and unsupervised variants of ML, RL agents can learn in real-time via observations obtained through online interactions with the environment. The agent is not designed to act; instead, the agent's behavior is reinforced through rewards. Undesirable actions performed by the agent are penalized, whereas desired actions by the agent are rewarded. The agent's purpose is to maximize the reward over a set length of time; once that time has passed, the agent is inclined to exhibit behaviors that will result in a good reward. While conventional RL performs well for systems in discrete state spaces, it is hard to apply it to continuous state spaces. Recently, deep learning and RL principles have been used in conjunction to solve large-scale optimal control problems with continuous observation spaces. Neural networks are used as function approximators when the observation space is too large to be completely known.

1.2. Cyberattacks

Cyber physical systems (CPSs) are vulnerable to cyberattacks. There are two typical cyberattacks, i.e., denial-of-service (DoS) and deception attacks. DoS attacks are tactics that obstruct data distribution or force the inactivation of specific control system components. For example, an adversary prevents communication of a LiDAR sensor with the control system in an AV. DoS attack may be deployed to prevent self-driving vehicles from identifying objects, roads, and safety signs. This may cause a vehicle's braking system to fail, leading the vehicle to halt abruptly or fail to stop as needed. DoS attacks are typically characterized by two parameters: DoS frequency and DoS duration. Deception attacks are methods in which an attacker alters the data used by a CPS. The attacker sends fraudulent data directly to the target system or decodes input data and injects it with fraudulent data. An attacker taking control of a sensor and purposely changing the readings is an example of a deception attack. Researchers in [2] have deceived a LiDAR-based AV into detecting artificial impediments to influence its driving decisions. Deception attacks can be categorized as adversarial attacks and replay attacks. Adversarial attacks work by modify slightly the input data that may not be perceptible to humans but may result in undesirable system behavior. For instance, it is shown in [3] that changing just one pixel in an image may misclassify data in deep neural networks. Researchers in [4] demonstrated that adversarial attacks and fault injection on a deep learning based end-to-end autonomous driving strategy could lead to erroneous driving decisions and severely jeopardize safety. Replay attacks are strategies in which an attacker uses previously recorded data as input to the system to disrupt it. The attacker captures a series of actual sensor measurements and then uses them later during an attack to replace the current measures to deceive the system. This type of attack is tough to detect because it is hard to differentiate the replay inputs from actual current data. Cyber physical attacks are not limited to the abovementioned categories and are comprehensively categorized in [5]. Most studies focus on the effects of such threats on traditional autonomy, with several ML agents working in tandem. This work investigates the effects of such threats on a DRL based end-to-end fully autonomous systems.

2. Learning Algorithm

This paper uses a deep Q-learning algorithm to obtain a self-driving strategy for an AV in the CARLA simulator. CARLA is an open-source simulation platform built with Unreal Engine that allows for the simulation of realistic driving environments, making it ideal for training self-driving agents. Multiple sensors are available in CARLA, such as collision detectors, depth cameras, Inertial Measurement Unit (IMU), LiDAR, and RGB. Deep Q-network (DQN) is a deep variation of Q-learning algorithms. DQNs use convolutional neural networks (CNNs) to process the image observations by extracting unique features. Generally, CNNs are used to classify data, but in DQNs, they produce Q-values for all possible actions for any state observation. The CNNs use convolution layers to extract features from the input images. The output of the convolution layers is flattened into a one-dimensional array and fed into fully connected layers. The output from the fully connected layers is the Q-values corresponding to the defined actions.

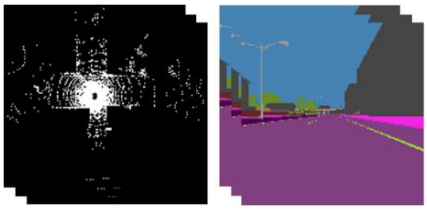


Fig. 1. Network Inputs.

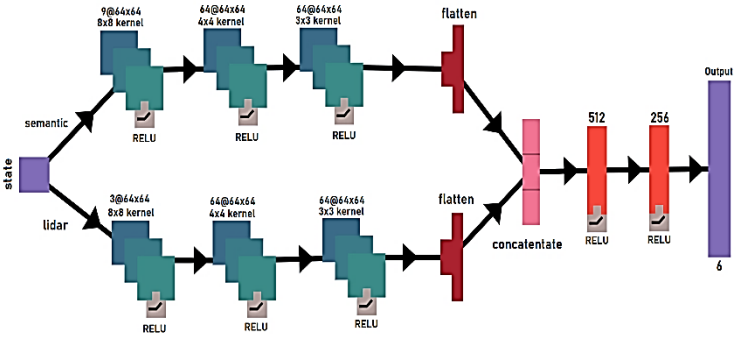


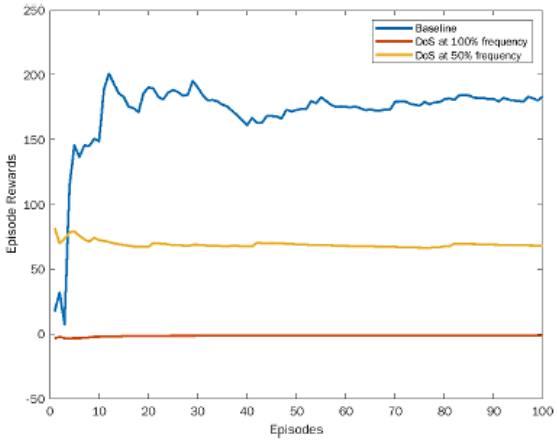
Fig. 2. DQN Architecture.

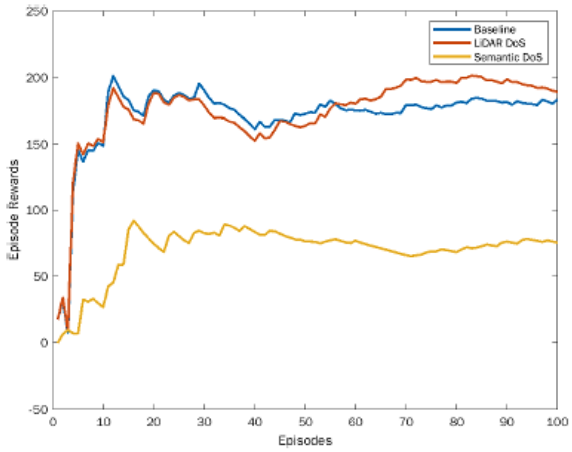
In our DQN implementation, we use a pair of CNNs in parallel. One extracts features from a birds-eye view LiDAR image and the other from RGB images, as illustrated in Fig. 1. The network architecture is presented in Fig. 2. Both networks include three 64-layer convolution layers with kernel sizes of 8x8, 4x4, and 3x3. The CNNs output is concatenated and sent through a fully connected neural network to provide 6 Q-values as the output. These Q-values estimate the best policy for selecting actions from a discrete action space. A replay buffer saves the agent's transitions in memory at each environmental step during training, which improves sample efficiency and the generalization of policies. It disrupts the correlation between successive samples which makes the agent learns efficiently. The training aims to find the best way to estimate the Q-function to be a near-optimal action-value function.

We designed the reward function for our DQN agent to minimize collisions and encourage the vehicle to keep moving. Therefore, we use distance to obstacles, vehicle speed, steering rate, and collision as the function arguments. The equation below describes the reward function used as $r_t = -200r_{col} + r_{radar} + r_{speed} + r_{cont} + r_{steer} + r_{proxi}$, where, r_{col} is the reward for collision, r_{radar} is associated with distance to an obstacle, r_{speed} is the reward corresponding to the vehicle's velocity, r_{cont} is a small constant reward given to encourage longer episode durations, r_{steer} is a reward given to discourage driving around in circles or turning constantly, and r_{proxi} is a reward given based on proximity to the edge of the road to encourage the agent to stay on the road. r_{col} is 1 if the agent crashes and 0 otherwise. r_{radar} is -1 if an obstacle is within three meters of distance and 0 otherwise. The speed reward is a quadratic function, i.e., $r_{speed} = -0.0017v^2 + 0.1667v - 1$, which returns a small negative value if the vehicle is stationary or going too fast, and a positive value otherwise. The steer reward is $r_{steer} = -\alpha^2$, where $\alpha \in [-1,1]$ is the steering ratio. The proximity reward is -0.5 if a vehicle accelerates towards an out of road element in proximity, 0.5 if it slows down or comes to a stop when heading towards such element, and 0.25 otherwise.

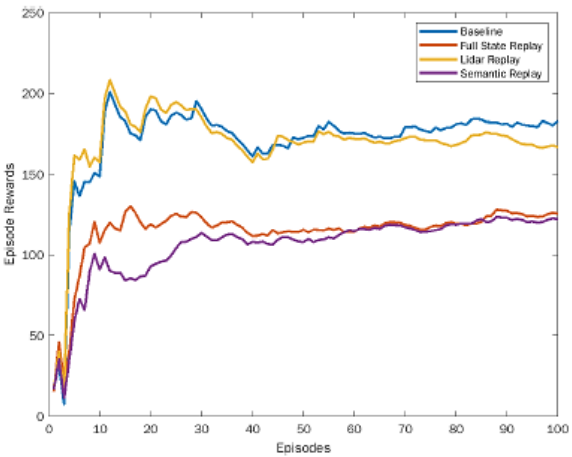
3. Resilience Against Cyberattacks

To study the ramifications of cyber-physical threats on AVs, we applied an autonomous driving strategy through a trained DQN and subjected it to different cyberattacks in an urban scenario.





(a) Full state DoS attack (b) DoS attack on individual sensors



(c) Replay Attacks.

Fig. 3. Moving average reward plots for a DRL agent subjected to cyberattacks.

a) DoS Attack: We subject the self-driving agent to DoS attacks by disrupting the agent's sensor inputs at different DoS frequencies and assess what behavior would result from disrupting only some of the sensors. First, we disrupt all sensor data at 100% and 50% frequencies. Fig. 2(a) illustrates the moving average rewards obtained through a hundred episodes. When no data is available, the agent prefers to stay stationary to minimize its chances of collision—resulting in a low overall reward for a 100% DoS case. When the data stream is disrupted at a lower frequency, the vehicle exhibits a "stop-and-go" behavior resulting in slightly higher average rewards for 50% DoS frequency. We then expose the agent to similar disruption frequencies but for individual sensors. Fig. 2(b) illustrates the moving average rewards obtained for this experiment. The agent here exhibits more resilience to adverse behavior in this situation, as it can compensate for missing data from one data source. Our agent has learned to give

higher importance to semantic image data than LiDAR data. Thus, its performance is scarcely affected when only the LiDAR data is disrupted. When the semantic data is disrupted instead, the agent can still compensate for the missing information but is much less confident about its actions—resulting in lower driving speeds and reduced average rewards.

b) Deception Attack: We subject our autonomous agent to several replay attacks to observe the vehicle's behavior and rewards. Fig. 2(c) illustrates moving average rewards for deception attacks. A "stop-and-go" behavior of different degrees is observed when either of the sensor inputs is fraudulent. It can be attributed to the importance of each sensor in decision-making and conflicting state information. When a replay attack is performed only on LiDAR data, the vehicle's behavior is least affected, resulting in random slowdowns with otherwise equivalent to baseline performance. The replay data recorded consisted of driving on straight roads with a few turns at intersections. When either the semantic or full-state replay is used, the agent speeds up to drive straight, collecting higher rewards than the DoS attack before it crashes. Thus, resulting in positive but low average rewards. Semantic replay rewards are slightly lower than the full-state replay because the agent slows down due to information disparity.

Further Discussions

a) Reward Function: From the various attacks implemented on the vehicle, one major thing observed was the importance of the reward function when it comes to an RL algorithm's resilience against cyberattacks. The agent always seeks to maximize its reward. Through our experiments, we observed that the agent exhibited behaviors that were sure to increase the reward. When one of the agent's sensors is subjected to DoS attacks, the agent will slow down to avoid the substantial negative reward resulting from a collision. The autonomous agent was even more careful when taking turns. It would choose not to move when it sensed that it was close to an obstacle. Considering this, a reward function can be constructed to aid the agent in performing well when under a cyberattack.

b) Feature Extraction: We also subjected the sensors to various noises; Gaussian, salt and pepper, Poisson, and speckle noises. The rewards obtained were identical to the baseline, but the vehicle slowed just a bit in terms of behavior. This phenomenon can be attributed to the performance of the CNN; the convolution layers do a great job extracting features from the input images even in the presence of small amounts of noise. It also could be attributed to the semantic image data as it has a lower distribution of colors and intensity gradients. We gradually increased the intensity of the noise, and the agent still performs well until the image is almost unrecognizable.

4. Conclusion and Future Works

In this paper, we have used CARLA driving simulations to investigate the resilience of deep Q-learning algorithms for autonomous driving. Various cyberattacks were tested, including DoS and replay attacks. Simulation results demonstrate that cyberattacks on the LiDAR sensor have a minor impact on the DQN's performance; however, any attack on the semantic RGB sensor significantly impacts the DQN's performance. As a future work, the resilience of recurrent DRL algorithms will be investigated for continuous action spaces [6].

References

[1] Z. P. Jiang, T. Bian, and W. Gao, "Learning-based control: A tutorial and some recent results," Foundations and Trends in System and Control., vol. 8, no. 3, pp. 176–284, 2020.

[2] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on LiDAR-based perception in autonomous driving," Proceedings of the ACM Conference on Computer and Communications Security, pp. 2267-2281, 2019.

[3] J. Su, D. V. Vargas, and K. Sakurai, "One pixel attack for fooling deep neural networks," IEEE Transactions on Evolutionary Computation, vol. 23, no. 5, pp. 828–841, 2019.

[4] Piazzesi, N., Hong, M. and Ceccarelli, A., "Attack and fault injection in self-driving agents on the CARLA simulator–experiencerReport," International Conference on Computer Safety, Reliability, and Security, pp. 210-225, 2021.

[5] A. Khadka, P. Karypidis, A. Lytos, and G. Efstathopoulos, "A benchmarking framework for cyber-attacks on autonomous vehicles, " Transportation Research Procedia, vol. 52, pp. 323-330.

[6] L. Meng, R. Gorbet, and D. Kulic. Memory-based deep reinforcement learning for POMDP. International Conference on Intelligent Robots and Systems, 2021.

MMTC OFFICERS (Term 2020 — 2022)

CHAIR

Jun Wu
Fudan University
China

STEERING COMMITTEE CHAIR

Joel J. P. C. Rodrigues
Federal University of Piauí (UFPI)
Brazil

VICE CHAIRS

Shaoen Wu (North America)
Illinois State University
USA

Liang Zhou (Asia)
Nanjing University of Post and Telecommunications
China

Abderrahim Benslimane (Europe)
University of Avignon
France

Qing Yang (Letters & Member Communications)
University of North Texas
USA

SECRETARY

Han Hu
Beijing Institute of Technology
China

STANDARDS LIAISON

Weiyi Zhang
AT&T Research
USA

MMTC Communication-Frontier BOARD MEMBERS (Term 2016—2018)

Danda Rawat	Director	Howard University	USA
Sudip Misra	Co-Director	IIT Kharagpur	India
Guanyu Gao	Co-Director	Nanjing University of Science and Technology	China
Rui Wang	Co-Director	Tongji University	China
Lei Chen	Editor	Georgia Southern University	USA
Tasos Dagiuklas	Editor	London South Bank University	UK
ShuaiShuai Guo	Editor	King Abdullah University of Science and Technology	Saudi Arabia
Kejie Lu	Editor	University of Puerto Rico at Mayagüez	Puerto Rico
Nathalie Mitton	Editor	Inria Lille-Nord Europe	France
Zheng Chang	Editor	University of Jyväskylä	Finland
Dapeng Wu	Editor	Chongqing University of Posts & Telecommunications	China
Luca Foschini	Editor	University of Bologna	Italy
Mohamed Faten Zhani	Editor	University of Quebec	Canada
Armir Bujari	Editor	University of Padua	Italy
Kuan Zhang	Editor	University of Nebraska-Lincoln	USA
Bin Tan	Editor	Jinggangshan University	China