Machine Learning-based Efficient and Secure RSU Placement Mechanism for Software Defined-IoV

Sudha Anbalagan, Ali Kashif Bashir, *Senior Member, IEEE*, Gunasekaran Raja, *Senior Member, IEEE*, Priyanka Dhanasekaran, Geetha Vijayaraghavan, Usman Tariq, Mohsen Guizani, *Fellow, IEEE*

***Abstract*—The massive increase in computing and network capabilities has resulted in a paradigm shift from vehicular networks to the Internet of Vehicles (IoV). Owing to the dynamic and heterogeneous nature of IoV, it requires efficient resource management using smart technologies such as Software Defined Network (SDN), Machine Learning (ML), and so on. Road Side Units (RSUs) in Software Defined-IoV (SD-IoV) networks are responsible for network efficiency and offer several safety functions. However, it is not viable to deploy enough RSUs, and also the existing RSU placement lacks universal coverage within a region. Further, any disruption in network performance or security impacts vehicular activities severely. Thus, this work aims to improve network efficiency through optimal RSU placement and enhance security with a malicious IoV detection algorithm in an SD-IoV network. Therefore, the Memetic-based RSU (M-RSU) placement algorithm is proposed to reduce communication delay and increase the coverage area among IoV devices through an optimum RSU deployment. Besides the M-RSU algorithm, the work also proposes a Distributed ML (DML)-based Intrusion Detection System (IDS) that prevents the SD-IoV network from disastrous security failures. The simulation results show that M-RSU placement reduces the transmission delay. The DML-based IDS detects the malicious IoV with an accuracy of 89.82% compared to traditional ML algorithms.**

***Index Terms*—Internet of Vehicles, Machine Learning, Software Defined Network, RSU Placement, Intrusion Detection System.**

I. INTRODUCTION

Recent advances in the Internet of Things (IoT) technology have introduced a wide variety of processing devices like cameras, sensors, GPS, etc. Such sensors embedded in vehicles collect road information to communicate with other vehicles and have contributed to the advent of the Internet of Vehicles (IoVs) [1]. According to Gartner [2], the net global increase of autonomous vehicles will hit 7,45,705 units by 2023. By 2025, the massive economic impact produced by IoV has projected between $210 and $740 billion annually.

The exponential growth in computing and communication systems for IoV enables driving assistance and information sharing among them [3]. Besides, smart technologies like Virtual Reality (VR), and self-driving based applications, process large amounts of data, requiring a high degree of network processing and communications. Such delay-sensitive and high computation demand a new orientation in designing vehicular networks. These demands can be readily satisfied using future technologies like Distributed Machine Learning (DML), Software Defined Networking (SDN), and so on [4]. Software Defined-IoV (SD-IoV) meets high computing demands by providing flexibility in network management and data communication control. In SD-IoV, the data and control planes are separated with the aid of a centralized SDN controller [5].

Apart from network flexibility, performance plays a vital role in improving the Quality of Service (QoS) [6]. In the SD-IoV network, there are two modes of communication, namely: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication [7]. Road Side Units (RSUs) in SD-IoV are infrastructure nodes used for communicating information such as road hazard alerts, traffic, or weather updates to the vehicles. RSUs play a significant role in V2I communications as follows: i) distributing vital information to vehicles, (ii) transmitting received messages to specific recipients, and (iii) offering internet access to the vehicles in their range [8].

However, RSU needs high installation cost and maintenance cost in the IoV environment, demanding a balance between network coverage and deployment costs [9]. Especially in urban cities, massive deployment of RSUs can be very costly to efficiently cover the entire geographical area. Thus, RSU deployment critically impacts Capital Expenditure (CapEx) and Operational Expenditure (OpEx). Moreover, the delay in IoV depends on the number and location of available RSUs in the network [10].

Also, security is a vital aspect of the design of an IoV network. In SD-IoV, vehicles distribute traffic safety warnings to other vehicles, and any security breach results in catastrophic losses [11]. Also, compromised vehicles degrade the performance by sending false information to the network and RSU or disclose critical information to the attackers. Thus it is crucial to detect the security violation by vehicles at the ear-

Sudha Anbalagan is with the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India. (e-mail: sudha.anbazhagan@gmail.com).

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, UK. (e-mail: dr.alikashif.b@ieee.org).

Gunasekaran Raja, Priyanka Dhanasekaran and Geetha Vijayaraghavan are with the NGNLab, Department of Computer Technology, Anna University, Chennai, India. (e-mail: dr.r.gunasekaran@ieee.org, priyankasekard2511@gmail.com, geethu15@gmail.com).

Usman Tariq is with the Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia. (e-mail: u.tariq@psau.edu.sa).

Mohsen Guizani is with the Computer Science and Engineering Department, Qatar University, Doha, Qatar. (e-mail: mguizani@ieee.org).

liest. Motivated by this finding, the proposed RSU placement algorithm provides sufficient coverage with a limited number of RSUs. It improves network performance by reducing the transmission delay of vehicular communication. Further, the proposed DML-based Intrusion Detection System (IDS) in the SDN actively detects the malicious IoV and protects the network.

The contributions of this article are summarized as follows:

- An efficient Memetic-based RSU (M-RSU) placement algorithm for SD-IoV is proposed to minimize the network transmission delay. On average, the M-RSU algorithm reduces the delay by 42% and 11% compared with D-RSU [12] and GARSUD [13] algorithms, respectively.
- The M-RSU placement algorithm is also enhanced using the received signal strength to avoid signal degradation in urban areas, thereby improving the overall deployment coverage.
- An efficient DML-based IDS is also proposed to detect vehicles' malicious activity with high accuracy and less false alarms. The detection accuracy of the IDS is 89.82%, thus offering a secure SD-IoV network.

The rest of this paper is structured as follows: Section II discusses the existing literature related to RSU placement and ML-based IDS for SD-IoV. The overview of the SD-IoV and the necessary preliminaries are presented in Section III. The M-RSU placement algorithm is detailed in Section IV. Section V discusses the DML-based IDS used in the SD-IoV. Implementation and result analysis are provided in Section VI. Finally, the work is concluded in Section VII.

II. RELATED WORK

Machine Learning can mine knowledge from the given data and then use the acquired knowledge to control an agent's actions. ML strategies are majorly used in data-driven problems like optimization, classification, and so on [14]. IoV devices produce large quantities of data, and thus data-driven ML-based analytics aids in efficiently and securely managing the resources in the network [12]. Moreover, the optimal location for infrastructure like RSU in the IoV network is crucial, as RSUs deployed in a region with low vehicle coverage lead to under-utilization of available network resources.

In [15], DynLim is proposed, which uses a profit density function to maximize the RSU's utility and Integer Linear Programming (ILP) model to minimize the delay in a highway scenario. When this technique is applied to the urban environment, however, there is a deterioration of the network's performance. This problem is alleviated in [16] using a utility-based deployment model that aids in delay-tolerant applications. However, this model is not suitable for low vehicle density, as the transmission delay increases due to multi-hop communication between the vehicles.

Some of the literature works approach the RSU placement problems mathematically. In [17], the RSU placement problem is treated as the shortest path problem and solved using the ILP model. In [18], the placement uses a mathematical model based on the relationship between the delay and distance between RSUs. Bio-inspired algorithms, a branch of artificial intelligence, are also used for RSU placement optimization. For example, in [13], [19], the preliminaries of bio-inspired algorithmic operations like crossover, mutation, and replacement are discussed in detail and use a genetic algorithm to optimize the RSU placement of a fitness function based on message delay. A particle swarm optimization technique is used to minimize the deployment cost of both RSU and sensor nodes [20]. However, this RSU placement technique does not address the cross-layer challenges in a hybrid network. The authors used delay bounds, end-to-end backlog [21], and delta network parameters [22] as an efficiency measure of RSU placement to evaluate the QoS.

Concerning the security of IoV, various works based on cyber-physical systems like anomaly detection and IDS are proposed. Game-theory models are used to design IDS but lead to high computation complexity [23]. Alternatively, ML-based algorithms like logistic regression [14], naive bayes [24] are frequently used in IDS. Furthermore, the reputation and rule-based anomaly detection suffer from high false alarm generation and detect only the known attacks [25]. Support Vector Machine (SVM)-based IDS detects the attacks with high detection accuracy but requires high computational power [26]. In [27], the IDS state gets switched between active and idle using the Bayesian method to conserve power. In an idle state, however, the IDS cannot detect attacks and lead to a security loop-hole. Alternatively, [28] uses a hybrid ML approach by combining SVM and dolphin swarm optimization to detect network attacks, but such approaches are computationally complex.

To summarize, most of the existing RSU placement algorithms suffer from poor network performance and lack applicability towards versatile road scenarios. The existing IDS are predominantly in-vehicle IDS and therefore have a low detection accuracy due to less computational power and storage. The SD-IoV mitigates these problems through a combination of efficient RSU placement and DML- based IDS. The RSU placement algorithm optimizes network performance through improved coverage and reduced transmission delay. DML-based IDS detects the malicious activity of nodes thereby securing the network.

III. SOFTWARE DEFINED-IOV FRAMEWORK OVERVIEW

IoV technology in Intelligent Transportation Systems (ITS) improve road safety, traffic management, and infotainment applications. But, IoV has its challenges like high mobility, dynamic network topology, and so on. SDN is suitable for the dynamic nature of IoV by providing flexible routing among RSUs. Furthermore, the SD-IoV can provide increased uptime because an SDN controller manages the RSUs in the IoV through programmable routing protocols. Additionally, network efficiency can be enhanced by optimally placing RSUs, and this is a non-trivial task in an urban vehicular environment. Apart from the optimal placement of RSUs, it is equally important to detect compromised vehicles swiftly and secure

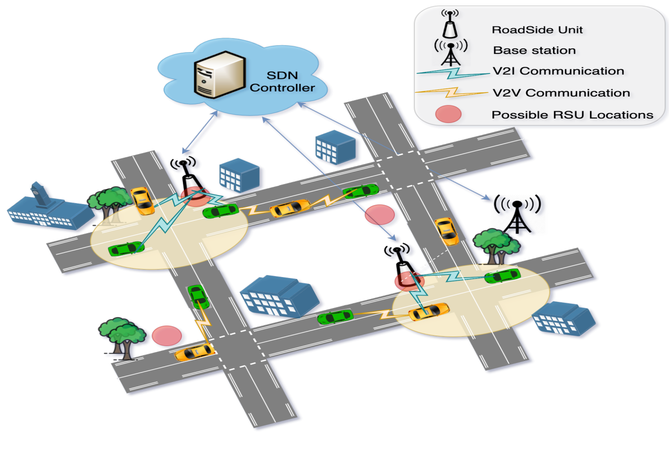

Fig. 1: System model of SD-IoV

the SD-IoV from catastrophic failures. These problems are addressed using the proposed M-RSU placement and DML-based IDS for SD-IoV. The proposed system model is, as shown in Fig. 1. The frequently used notations are listed in Table I.

A. Mobility Model

The vehicles in IoV are assumed to follow the Non-Homogeneous Poisson Process (NHPP) because of multiple peak hours in a city. The vehicular mobility is modeled as an NHPP with an arrival rate of $\lambda(t)$ where $t \geq 0$. The number of vehicles in road segment RS of length L at time t is represented as $N(L,t)$ and the expected number of vehicles $m(L,t)$ in RS at time t is

$$m(L,t) = E(N(L,t)) = \int_0^t \lambda(x)dx \tag{1}$$

The probability of n vehicles at time t in RS of length L is

$$P\{N(L,t) = n\} = \frac{[m(L,t)]^n}{n!}e^{-m(L,t)} \tag{2}$$

Let D_v be the transmission range of the vehicles and the probability there are no vehicles within D_v is expressed from Eq. (2) as

$$P\{N(D_v,t) = 0\} = e^{-m(D_v,t)} \tag{3}$$

TABLE I: List of Notations Used

Symbol	Description
t	Time
$\lambda(t)$	Arrival rate
L	Length of road segment
$N(L,t)$	Number of vehicles at time t
$m(L,t)$	Expected number of vehicles at time t
D_v	Transmission range of vehicles
P_s	Probability of successful multi-hop transmission
P_f	Probability of failure multi-hop transmission
$\rho_{0,n}$	Transmission delay for n vehicles
λ_p	Arrival rate of a packet
μ	Service rate of the channel
ρ_r	Average delay for V2I transmission
p	Packet size
R	Data rate of the channel

The transmission succeeds if there are vehicles in its transmission range D_v, that is capable of establishing V2V communication directly. Otherwise, the vehicles carry the message until the end of the road segment. For a road segment of length L, the multi-hop transmission succeeds if they are within each other's transmission range. As per Eq. (3), each vehicle has the probability $P\{N(D_v,t) = 0\}$ to disconnect from the V2V network. Let P_s be the successful multi-hop transmission probability in RS of length L, which is expressed as

$$P_s = (1 - e^{-m(D_v,t)})^{\frac{L}{D_v}} \tag{4}$$

$$P_f = 1 - P_s \tag{5}$$

where P_f represents the probability of failure of multi-hop transmission in the road segment of length L. The transmission delay for multi-hop transmission $(\rho_{0,n})$ in RS of length L is expressed as

$$\rho_{0,n} = \rho_0 \sum_{k=1}^{n-1} P_s^k + P_f \sum_{k=1}^{n-1} P_s^{k-1} \frac{D_{k,n}}{v} \tag{6}$$

where ρ_0, $D_{k,n}$ and v represents the transmission delay for one-hop communication, distance from k^{th} vehicle to n^{th} vehicle and average speed of the vehicles respectively. The vehicle that carries the message outside the deployed RSU coverage uses Base Station (BS) to report the incident (malicious activity or accident). Let us assume the packet's arrival rate (λ_p) and service rate of the channel (μ) follows an exponential distribution. The carrier sense multiple access mechanism is used, where the vehicle acquires the channel after random back-off. Once the channel is acquired, each vehicle begins message transmission, with a packet size of p. The packets in the vehicle buffer is serviced as $M/M/1$ queuing model. The average waiting time of the packet in the vehicle is expressed as

$$E[W_p] = \frac{\lambda_p}{\mu(\mu - \lambda_p)} \tag{7}$$

The average delay (ρ_r) from vehicle to infrastructure is obtained by including the packet transmission delay and is expressed as

$$\rho_r = E[W_p] + \frac{p}{R} \tag{8}$$

where $E[W_p], p, R$ represents average waiting time, packet size, and data rate respectively. Thus, the transmission attributes are mathematically formulated based on the vehicular mobility.

IV. M-RSU PLACEMENT MECHANISM

In SD-IoV, the RSU deployment's goal is to maximize the coverage area and minimize the message transmission delay. The placement of RSU is an offline design to create a network of RSUs in the urban IoV environment. Due to the low market penetration of IoV vehicles and the high deployment cost of RSUs, vehicular network design is generally restricted to use a limited number of RSUs for a given region. The delay defined in Eq. (6), (8) and coverage is incorporated in the memetic

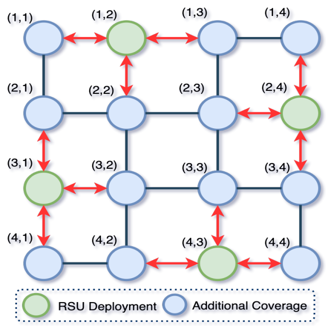

Fig. 2: RSU deployment in a 4 x 4 region

algorithm's fitness function, which is further elaborated in this section.

Let us consider a simple 4×4 road network for RSU deployment, where each intersection is a potential candidate location. Thus, there are 16 candidate locations for the RSU deployment. If the RSUs are deployed at locations highlighted in green, all the other locations are covered without any overlap, as demonstrated in Fig. 2.

In urban road networks, the RSU coverage is affected by the presence of obstacles such as buildings, trees, and so on. The interference due to these obstacles can be measured using a Received Signal Strength Indicator (RSSI) of the beacon message from a vehicle and is used to determine the coverage area of RSU. Thus, the RSU coverage area is the distance range in square meters, within which the RSSI is above a given threshold. This distance range is represented as a polygon (δ) specifying its coverage distance from all the road segments connecting it. If R number of RSUs available, then each RSU (i) has its polygon (δ_i) that covers a specific range in a given region in square meters. An efficient RSU placement strategy optimizes the coverage area by minimizing its overlap among RSUs. The coverage overlap of the RSU placement is the overlap among all the polygons (O_δ) is expressed as

$$O_\delta = \sum_{i=1}^{R} \sum_{j=i+1}^{R} O(\delta_i, \delta_j) \tag{9}$$

where $O(\delta_i, \delta_j)$ represents the overlapped area (i.e., intersection) between polygon δ_i and δ_j in square meters. Therefore the coverage (C_1) of RSU placement in a given region is expressed as

$$C_1 = \frac{\delta_c - O_\delta}{T_c} \tag{10}$$

where δ_c and T_c represents the total coverage area of all the polygons and the size of the region that need to be covered, respectively.

Another objective (C_2) of RSU placement is to reduce the transmission delay ($\rho_r, \rho_{0,n}$) in reporting the incident. Let us consider N number of scenarios (accident or malicious activity) that occur in an urban road network. The delay for V2V communication delay is calculated using the Eq. (6) and Eq. (8) is used to calculate the V2I communication delay. Thus, the objective function (C_2) of this problem is represented as

$$C_2 = N.\frac{100}{\sum_{i=1}^{N}(\rho_r(i) + \rho_{0,n}(i))} \tag{11}$$

Thus, by combining both objectives (C_1 and C_2) for solving the RSU placement problem in an urban scenario, the Fitness (F) function of the memetic algorithm is formulated as

$$F = Max(w_1 C_1 + w_2 C_2) \tag{12}$$

where the parameters w_1 and w_2 ranges from 0 to 1, which governs the control over the function C_1 and C_2 respectively.

In the M-RSU placement algorithm, a bio-inspired solution is used to efficiently place the RSUs in the given region, with k candidate locations. The M-RSU placement algorithm chooses

Algorithm 1 M-RSU Placement Algorithm

Input: Possible Location $L = L_1, L_2, L_3, \ldots, L_k$, Number of RSUs available R, Number of generation G, Offspring size n
Output: Set of R locations

Generate initial population of size G
$\alpha_c, \alpha_m \rightarrow$ Probability of crossover and mutation respectively
$\beta_c, \beta_m \rightarrow$ Index of crossover and mutation respectively
$\gamma_c, \gamma_m \rightarrow$ Random number between 0 and 1
while G not reached **do**
  for $i = 1$ *to* n **do**
    S_i = Selection(G)
  end for
  if $\gamma_c \geqslant \alpha_c$ **then**
    for $i = 1$ *to* $n/2$ **do**
      β_{ci} = index(Diff(S_i, S_{i+2}))
      β_{ci+2}= index(Diff(S_{i+2}, S_i))
      $S_i^{'}$, $S_{i+2}^{'}$=crossover(S_i, S_{i+2}, β_{ci}, β_{ci+2})
    end for
  end if
  if $\gamma_m \geqslant a_m$ **then**
    for $i = 1$ *to* n **do**
      β_{mi} = index(Diff($S_i^{'}$, S_u))
      β_{mu} = index(Diff(S_u, $S_i^{'}$))
      $S_i^{'}$=mutation($S_i^{'}$, S_u, β_{mi}, β_{mu})
    end for
  end if
  Local search replacement (L)
  for $i = 1$ *to* n **do**
    if $F_i^{'} > F_i$ **then**
      Replace S_i with $S_i^{'}$ in the population
    else
      S_i remains in the population and $S_i^{'}$ rejected
    end if
  end for
end while
return the set of locations

the optimal position for RSU deployment in a feasible time. Input parameters for the M-RSU placement algorithm include a set of possible candidate locations, number of RSUs to be deployed, size of the offspring, and a number of generations. The memetic algorithm is similar to the traditional genetic algorithm but differs by incorporating local search to avoid local optimum. The proposed M-RSU placement algorithm uses the fitness function (F), as given by Eq. (12), to place RSU strategically by optimizing the RSU coverage area and transmission delay. Steps 1 through 4 of Algorithm 1 specify the initial solution space generated from the possible locations, crossover and mutation probability, and their respective index and random numbers, respectively. Step 7 selects the solutions for M-RSU from the available population. The crossover operation is performed from steps 9 through 15, where the index of unique elements in each solution is obtained and gets interchanged. Similarly, the mutation occurs from steps 16 to 22, replacing the solution's element using a global set of locations.

At step 23, the local search replacement function (L) replaces the minimum δ value in the solution with the maximum value in the global location for C_1. The fitness value of the solution obtained in each iteration is calculated. Step 25 indicates that if the maximum fitness value is present in the current population, it is selected for the next generation. This algorithm iterates until it reaches the specified number of generations. The set of R locations are returned as output from the M-RSU algorithm, thereby achieving maximum RSU coverage with minimal transmission delay.

V. DISTRIBUTED MACHINE LEARNING BASED IDS FOR SD-IoV

In centralized ML techniques, the network traffic of the IoV network is monitored and sent to the centralized learning node that trains the neural model. For DML, each node has its network data and performs the ML steps to obtain its model. The global model is obtained by aggregating the model parameters of all the nodes in the network. The DML performs data parallelism to reduce the storage space requirement of IDS. The DML is scalable for large input datasets; as the dataset increases, the system's accuracy also increases.

The SD-IoV uses a DML-based IDS algorithm to detect vehicles' malicious activity by monitoring the network traffic data. In the IDS, the RSUs receive the SDN's global model parameters and locally create the ML model using its training data. The updated model parameter of RSUs is sent to the SDN, where the model aggregation is performed, resulting in a new global model. The process of DML continues until the termination condition is reached. Thus, the DML technique preserves training data privacy by exchanging the model parameters instead of data and meets the storage and computation demands of IDS.

Algorithm 2 of DML-based IDS receives the input as network traffic data and outputs the model parameter or intrusion detection alarm. In step 2, the SDN controller initializes the set of weights ω_0 for the global model. Step 3 to 10 iterates the updation of the global model up to the threshold (th). In step 4, the random set of RSUs are selected, where R and C represents the number of RSUs and $C \in (0, 1]$ a hyperparameter, respectively. In step 7, each RSU (k) receives the SDN weights and therefore performs RSU update procedure. Step 9 completes the aggregation of model parameters (ω^k_{i+1}) from all the selected RSUs. Step 13 of the RSU update procedure, pre-processes, and split the training data into batches of size B. In steps 14 to 23, each selected RSU iterates up to local epoch (t), thereby building the model based on the received weights and local training data. From step 17 to 20, the RSU uses the trained model to detect a vehicle's malicious activity. If any malicious activity is found, then it sends the intrusion alarm to the respective authority. The RSU updates the local weights using its training data as per step 21. Finally, the local updated weight (ω) is sent to the SDN controller for model aggregation.

Algorithm 2 DML-based IDS for SD-IoV

Input: Network traffic data
Output: Model parameter or Intrusion alarm

```
1:  procedure SDN_update:
2:  Initialize ω_0
3:  for i = 1, 2, .., th do
4:      m ← max(R.C, 1)
5:      S_i = select random set of m RSUs
6:      for each RSU k ∈ S_i do
7:          ω^k_{i+1} ← RSU_update(k, ω_i)
8:      end for
9:      ω_{i+1} ← Σ_{k=1}^{R} (n_k / n) ω^k_{i+1}
10: end for
11: end procedure

12: procedure RSU_update (k, ω_i):
13: Pre-process and split the data into batches of size B
14: for i = 1, 2, ..t do
15:     for each batch b ∈ B do
16:         Build the model using received weights
17:         Use the trained model in the IDS
18:         if IDS in RSU detects intrusions then
19:             Send Alarm()
20:         end if
21:         ω ← ω − η∇F_k(ω)
22:     end for
23: end for
24: return ω to the SDN controller
25: end procedure
```

Each RSU with a fixed learning rate (η) receive the global model parameters and the gradient descent (g_i) [29] using the local training data is calculated as follows:

$$g_i = \nabla F_k(w_i) \tag{13}$$

where $F_k(w_i)$ represents the estimation of weight based on the loss value obtained for each data in training set. The local

TABLE II: Simulation Parameters

Parameter	Value
Area Size	500 m x 500 m
Number of Vehicles	100 - 400
Vehicle Velocity	80 - 120 kmph
Number of RSUs	1 - 20 RSUs
Direction	Bi-directional
RSU, Vehicle Transmission Range	300 m
RSU, Vehicle Interference Range	600 m
Channel Mode	Wireless
Interface Queue	Drop tail/ Priority queue
Propagation Model	Two ray ground
Routing Protocol used	AODV protocol
MAC Type	IEEE 802.11
Antenna Mode	Omni-directional
Agent Type	TCP
Simulation Time	500 sec
Representation	Numerical
Crossover Type	1-point cross over
Probability of Mutation	1 gene/ individual (average)
Parent Selection	Tournament $k = 2$
Population Size	8
Initialization	Random
Number of Generations	21
Number of Executions	5

weight update for each selected RSU is specified as

$$\forall k, w_{i+1}^k \leftarrow w_i - \eta g_i^k \tag{14}$$

The SDN controller updates the weights of the global model w_{i+1} by aggregating the weights w_{i+1}^k of the selected RSUs. The computational complexity of the DML-based IDS is measured as $O(\frac{\sum_1^{th}\sum_k^m(t)}{R})$, where th, m, R and t represents a global model threshold, number of selected RSUs at each global iteration, number of deployed RSUs and local epoch respectively. Thus, the DML-based IDS prohibits any malicious vehicle from attacking the SD-IoV and prevents network performance from deteriorating due to disruptive activities.

VI. IMPLEMENTATION AND RESULTS

This section presents the experimental analysis of RSU placement and DML-based IDS performance in the SD-IoV environment. A detailed list of the parameters used in the M-RSU placement algorithm is shown in Table II. The M-RSU placement algorithm uses the vehicular traffic traces of Chandigarh in India, extracted from OpenStreet Maps (OSM) and visualized in Simulation of Urban Mobility (SUMO), as shown in Fig. 3. Each intersection represents the possible RSU location in the given region. Nevertheless, even in a small area with a minimal number of RSUs, it is impractical to assess every possible combination of candidate locations for RSU placement. For example, if a region has 200 locations with 5 RSUs to be placed, then there are 2.5357e+9 different RSU placement possibilities. The proposed M-RSU placement algorithm finds the optimal locations to deploy RSUs by selecting the best solution with the maximal fitness value. The RSU coverage polygon is computed using the RSSI from all the road segments intersecting the RSU location. The coverage polygon is established with a received RSSI threshold value of -94db or greater.

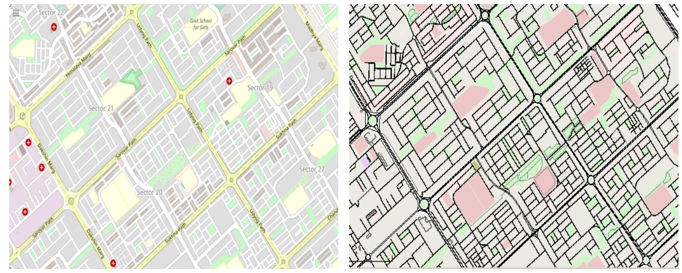

Fig. 3: OSM and SUMO road network of Chandigarh in India

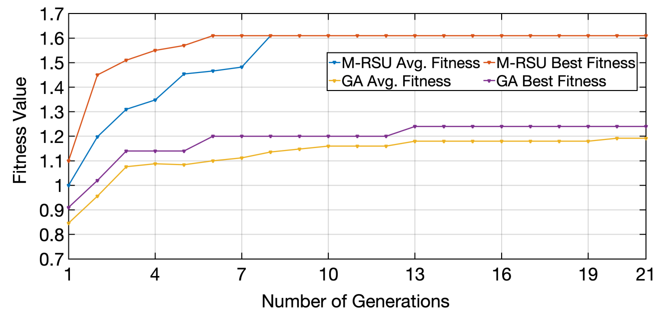

Fig. 4: Fitness value comparison of RSU placement algorithms

The M-RSU placement strategy initializes the population by randomly selecting the locations in the given region. Each RSU location computes its polygon and is stored to avoid recomputation. The coverage overlap and fitness value of the selected solution are computed, as formulated in Eq. (10). The transmission delay is calculated based on the vehicular mobility with N=3, where N denotes the average number of incidents in a given region. The parameters w_1 and w_2 control the trade-off between the coverage and delay objectives of RSU placement. If w_1 is zero, then placement occurs based on the delay minimization, and if w_2 is zero, then RSUs are placed based on the coverage maximization. Therefore based on w_1 and w_2, the M-RSU finds the location having increased coverage and decreased communication delay. M-RSU uses local search for elitism and both w_1, w_2 as 0.5. The M-RSU placement is compared with Genetic Algorithm (GA) [13] using five executions, and each run spans over 21 generations. The best and average fitness analysis is shown in Fig. 4 and observed that the M-RSU converges to the best fitness within 10 generations. Even in the best and average case, the existing GA algorithm generates inefficient results compared with the proposed M-RSU, and it does not converge until the last iteration.

The M-RSU placement algorithm is also compared with the existing Density-based RSU placement (D-RSU) [12] and GA for RSU Deployment (GARSUD) [13] by varying the number of vehicles and RSUs. As shown in Fig. 5, it is inferred that the proposed M-RSU placement reduces the reporting time approximately by 42% and 11% on an average compared to the D-RSU and GARSUD, respectively.

The V2I delay for a vehicle in a road segment near RSU at

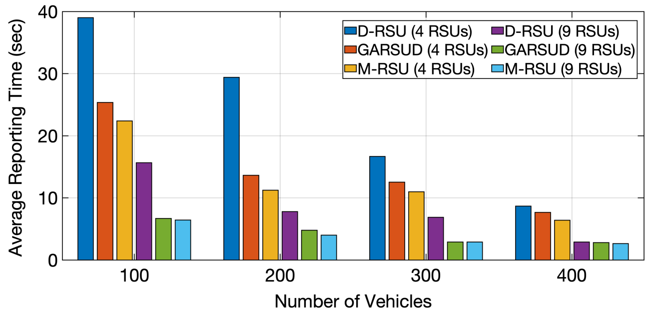

Fig. 5: Reporting time comparison of RSU placement

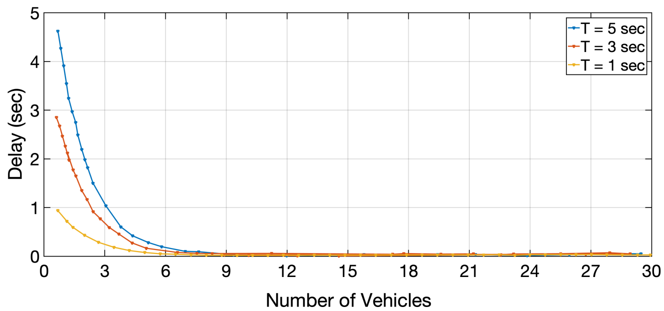

Fig. 6: V2I Average delay for various time intervals

the different waiting time (T) in seconds (T=1, T=3, T=5) is plotted in Fig. 6 and it is found that the increase in vehicular density decreases the delay. The increased vehicle density specifies that the vehicle uses V2V communication for its transmission, reducing the delay even with the long waiting time. The M-RSU placement covered the maximum area in the network, as shown in Fig. 7, and noticed that the coverage and overlap in a given region vary with the number of RSUs. It is observed that by increasing the number of RSUs in the network, increases the coverage with minimal overlap.

The DML algorithm used in the IDS is simulated using python, and the models are assessed using the following evaluation metrics: accuracy, precision, recall, and F1-score. Fig. 8 shows the evaluation scores of the models used in IDS. All the classifiers detect the malicious vehicle with an accuracy greater than 97% using the training data. In Fig. 9, the evaluation metrics of various classifiers using testing data are presented. The DML-IDS model detects the malicious vehicle with an accuracy of 89.82% and performs better than other ML models.

The DML-based IDS minimizes its loss function using the received model parameters from the SDN controller. In Fig. 10, the DML-based learning curve of RSU is shown and it uses the binary cross-entropy loss function. Based on the updated global model function, the RSU minimizes its loss, thereby improving detecting the intruders in the network. Thus, the M-RSU placement in SD-IoV maximizes the coverage as well as minimizes the transmission delay. Further, the DML-based IDS detects the intruders with high accuracy, thereby enhancing network security.

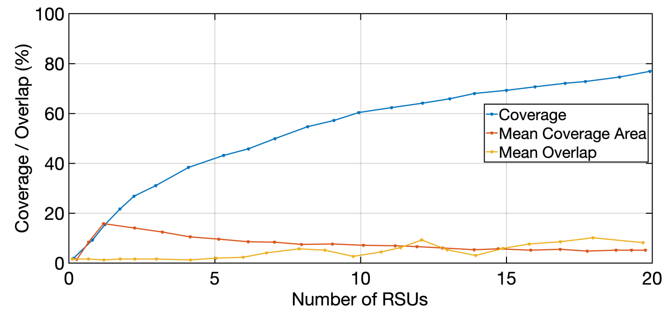

Fig. 7: Coverage comparison of RSUs

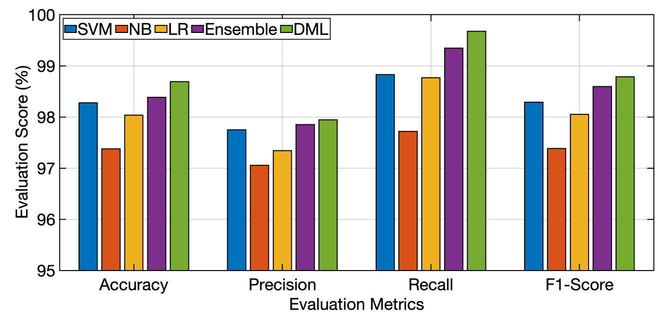

Fig. 8: IDS evaluation of training data

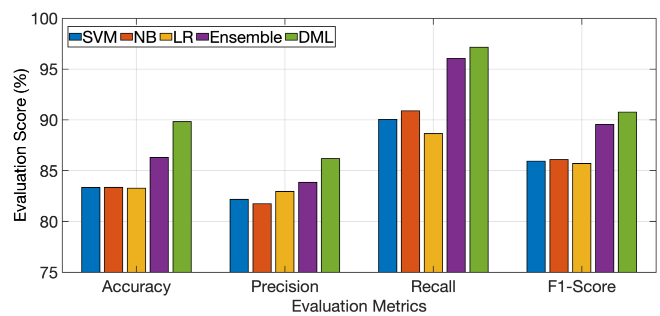

Fig. 9: IDS evaluation of testing data

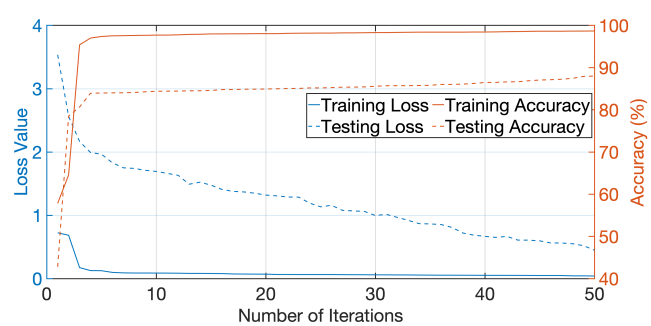

Fig. 10: DML-based learning curve

VII. Conclusion

In this paper, for an efficient RSU deployment, the M-RSU placement algorithm is proposed to determine the optimal position of the RSU. This algorithm improves the distribution of RSUs in a minimal number on any road map structure, from normal to sophisticated city layouts. An optimal RSU location reduces the message communication delay and improves coverage to the vehicles in a given region. Based on the simulation results on real-time traces, it is seen that the M-RSU algorithm performs much better on complex scenarios with a different number of RSU settings. The M-RSU based deployment has reduced the average V2I delay, which is especially suitable for safety applications that deal with emergency messages and communication-intensive applications. Additionally, security is provided by detecting malicious vehicles with DML-based IDS placed in the SDN controller. Compared to the other ML classifiers, the DML-based classifier has higher accuracy, making it suitable for the SD-IoV environment.

Acknowledgement

Gunasekaran Raja, Priyanka Dhanasekaran and Geetha Vijayaraghavan gratefully acknowledge support from NGNLab, Department of Computer Technology, Anna University, Chennai, India.

References

[1] A. Ali, L. Feng, A. K. Bashir, S. El-Sappagh, S. H. Ahmed, M. Iqbal, and G. Raja, "Quality of Service Provisioning for Heterogeneous Services in Cognitive Radio-Enabled Internet of Things," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 328–342, 2020.

[2] M. Rimol, "Gartner forecasts more than 740,000 autonomous-ready vehicles to be added to global market in 2023."

[3] S. Anbalagan, D. Kumar, G. Raja, and A. Balaji, "SDN assisted Stackelberg Game model for LTE-WiFi offloading in 5G networks," *Elsevier - Digital Communication and Networks*, vol. 5, pp. 268–275, 2019.

[4] G. Raja, P. Dhanasekaran, S. Anbalagan, A. Ganapathisubramaniyan, and A. K. Bashir, "SDN-enabled Traffic Alert System for IoV in Smart Cities," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1093–1098, 2020.

[5] G. Raja, A. Ganapathisubramaniyan, S. Anbalagan, S. B. M. Baskaran, K. Raja, and A. K. Bashir, "Intelligent Reward-Based Data Offloading in Next-Generation Vehicular Networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3747–3758, 2020.

[6] S. Anbalagan, D. Kumar, D. Ghosal, G. Raja, and M. V, "SDN-Assisted Learning Approach for Data Offloading in 5G HetNets," *Springer - Mobile Networks and Applications*, vol. 22, pp. 1–12, 2017.

[7] S. Anbalagan, D. Kumar, M. F. J, G. Raja, W. Ejaz, and A. K. Bashir, "SDN-assisted efficient LTE-WiFi aggregation in next generation IoT networks," *Elsevier - Future Generation Computer Systems*, vol. 107, pp. 898 – 908, 2020.

[8] G. Raja, S. Anbalagan, G. Vijayaraghavan, P. Dhanasekaran, Y. D. Al-Otaibi, and A. K. Bashir, "Energy-Efficient End-to-End Security for Software Defined Vehicular Networks," *IEEE Transactions on Industrial Informatics*, 2020. DOI:10.1109/TII.2020.3012166.

[9] N. Nikookaran, G. Karakostas, and T. D. Todd, "Combining Capital and Operating Expenditure Costs in Vehicular Roadside Unit Placement," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7317–7331, 2017.

[10] Z. Ahmed, S. Naz, and J. Ahmed, "Minimizing transmission delays in vehicular ad hoc networks by optimized placement of road-side unit," *Springer - Wireless Networks*, vol. 26, no. 4, pp. 2905–2914, 2020.

[11] G. Raja, S. Anbalagan, G. Vijayaraghavan, S. Theerthagiri, S. V. Suryanarayan, and X. W. Wu, "SP-CIDS: Secure and Private Collaborative IDS for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2020.

[12] J. Barrachina, P. Garrido, M. Fogue, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Road side unit deployment: A density-based approach," *IEEE Intelligent Transportation Systems Magazine*, vol. 5, no. 3, pp. 30–39, 2013.

[13] M. Fogue, J. A. Sanguesa, F. J. Martinez, and J. M. Marquez-Barja, "Improving Roadside Unit deployment in vehicular networks by exploiting genetic algorithms," *Applied Sciences*, vol. 8, no. 1, p. 86, 2018.

[14] E. Besharati, M. Naderan, and E. Namjoo, "LR-HIDS: logistic regression host-based intrusion detection system for cloud environments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 9, pp. 3669–3692, 2019.

[15] Z. Gao, D. Chen, S. Cai, and H. Wu, "OptDynLim: An Optimal Algorithm for the One-Dimensional RSU Deployment Problem With Nonuniform Profit Density," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 1052–1061, 2019.

[16] Y. Ni, J. He, L. Cai, J. Pan, and Y. Bo, "Joint Roadside Unit Deployment and Service Task Assignment for Internet of Vehicles (IoV)," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3271–3283, 2019.

[17] Y. Liang, Z. Wu, Y. Tian, and H. Chen, "Roadside unit location for information propagation promotion on two parallel roadways with a general headway distribution," *IET Intelligent Transport Systems*, vol. 12, no. 10, pp. 1442–1454, 2018.

[18] Y. Wang, J. Zheng, and N. Mitton, "Delivery delay analysis for roadside unit deployment in vehicular ad hoc networks with intermittent connectivity," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8591–8602, 2015.

[19] R. Gunasekaran, S. Siddharth, P. Krishnaraj, M. Kalaiarasan, and V. Uthariaraj, "Efficient algorithms to solve Broadcast Scheduling problem in WiMAX mesh networks," *Elsevier - Computer Communications*, vol. 33, pp. 1325–1333, 07 2010.

[20] C.-C. Lin and D.-J. Deng, "Optimal two-lane placement for hybrid VANET-sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7883–7891, 2015.

[21] Y. Hu, H. Li, Z. Chang, and Z. Han, "End-to-End Backlog and Delay Bound Analysis for Multi-Hop Vehicular Ad Hoc Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6808–6821, 2017.

[22] C. Silva, L. Silva, L. Santos, J. Sarubbi, and A. Pitsillides, "Broadening Understanding on Managing the Communication Infrastructure in Vehicular Networks: Customizing the Coverage Using the Delta Network," *Future Internet*, vol. 11, pp. 1–19, 2018.

[23] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for wireless sensor networks," *International Journal of Wireless Information Networks*, vol. 25, no. 4, pp. 399–421, 2018.

[24] K. Wang, "Network data management model based on naïve bayes classifier and deep neural networks in heterogeneous wireless networks," *Elsevier - Computers & Electrical Engineering*, vol. 75, pp. 135–145, 2019.

[25] T. Bouali, S.-M. Senouci, and H. Sedjelmaci, "A distributed detection and prevention scheme from malicious nodes in vehicular networks," *International Journal of Communication Systems*, vol. 29, no. 10, pp. 1683–1704, 2016.

[26] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," *Elsevier - Expert Systems with Applications*, vol. 50, pp. 40–54, 2016.

[27] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1143–1153, 2016.

[28] S. Sharma and A. Kaul, "Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET," *Elsevier - Vehicular Communications*, vol. 12, pp. 23–38, 2018.

[29] H. McMahan, E. Moore, D. Ramage, and B. A. y Arcas, "Federated learning of deep networks using model averaging," *ArXiv*, vol. abs/1602.05629, 2016.