Decentralized Authenticated Traffic Preemption Protocol

Nuthan Suryanarayana Raju Anusuri
Dept. of Computer Science and Engineering(Cyber Security)
SRM Institute of Science and Technology, Tiruchirappalli
Tiruchirappalli, India
anusurinuthan@gmail.com

Sirigiri Spoorthi
Dept. of Computer Science and Engineering(Cyber Security)
SRM Institute of Science and Technology, Tiruchirappalli
Tiruchirappalli, India
ss8464@srmist.edu.in

Dr. E Mohanraj
Professor, School of computing
SRM Institute of Science and Technology, Tiruchirappalli
Tiruchirappalli, India
mohanraj.e@ist.srmtrichy.edu.in

***Abstract*— Ambulances, fire trucks, and police cars are all examples of emergency vehicles that are greatly delayed by traffic jams at intersections. Traditional traffic signal preemption systems use optical emitters, infrared signals, or centralized GPS-based communication systems. These systems have problems like needing a line of sight, having a long delay, and being easy to spoof. This paper puts forward a Decentralized Authenticated Traffic Preemption Protocol (DATPP) that allows for secure and real-time prioritization of emergency vehicles at traffic intersections through the use of Vehicle-to-Infrastructure (V2I) communication and cryptographic authentication methods.**

The decentralized edge-computing design contains elements that will allow each intersection to include a Roadside Unit (an RSU is a device which will authenticate an emergency vehicle locally by using cryptographic tokens generated by HMAC algorithms and rolling counters). When an emergency vehicle is authenticated by the RSU, the RSU will dynamically modify the traffic light phases to give the emergency vehicle the best possible route while ensuring a safe continuation of traffic flow. The proposed protocol will also include a conflict resolution algorithm to handle cases where multiple emergency vehicles are attempting to get through the same intersection at the same time.

***Keywords*— Emergency Vehicle Preemption, Intelligent Transportation Systems, Vehicle-to-Infrastructure Communication, Traffic Signal Control, Cryptographic Authentication, Smart City Transportation.**

I. INTRODUCTION

Cities deal with rising traffic congestion on the roadways, which has an immediate impact on all three types of emergency services (police, fire service, and ambulance), because they all must use roadways to get to their designated locations. When emergency vehicles arrive at an intersection that has traffic lights and are required to wait for the lights to change, or traversing through a lane that is backed up due to congestion, it creates a bottleneck that forces the emergency vehicle to lose valuable time. Therefore, reducing delayed time to traverse an intersection is important for better public safety and more efficient emergency response.

Traffic signal preemption (TSP) system technology has come about because of this need to provide an emergency vehicle priority through intersection control. Current systems use optical emitters, infrared transmitters or acoustic sirens as their primary means of triggering a change in the traffic signal response. However, there are inherent issues associated with the above technologies which include the ability of the technology to utilise visual contact to trigger traffic signal changes, susceptibility to weather and no security to ensure that only authorized emergency vehicles have access to TSP systems.

New technology tries to upgrade current methods for managing the traffic system by including GPS tracking and centralized cloud-based traffic planning systems. These solutions increase coverage, but have new problems, such as delayed response time on the network, high system installation costs and being susceptible to loss of overall management if the centralized server is no longer accessible.

II. LITERATURE REVIEW

A. *Vehicular Ad-hoc Networks (VANET)*

VANETs allow for vehicle-to-infrastructure communication, which will ultimately increase traffic efficiency and safety. Hartenstein and Laberteaux examined the possibilities of combining the use of Dedicated Short Range Communications (DSRC) and various types of data exchanged in order to achieve real-time information about traffic conditions, accident location, and notify emergency services regarding vehicles in need of assistance. Open access issues must be addressed as part of the overall VANET implementation process. Additionally, a secure network level coordination mechanism will be needed to provide access control to vehicles, equipment, and communication relation to VANETs.

B. *Vehicle-to-Vehicle & Vehicle-to-Infrastructure Communication*

According to Santa et al., the proposed architecture integrates V2V (Vehicle-to-Vehicle) communication systems with V2I (Vehicle-to-Infrastructure) communication systems in a single framework that enables vehicles to share real time traffic data amongst other vehicles and traffic infrastructure (e.g., stoplight, traffic signs, etc.). Use of this type of architecture allows for better management of traffic and increased safety by providing more reliable communication networks while enabling secure transmission protocols to provide evidence of the authenticity of the data transmitted between vehicles and the transmission of these data between vehicles and the traffic infrastructures to which they are connected.

C. Emergency vehicle signal preemption systems

A research study by Teng et al. assessed how preemption of stoplights affects urban traffic flow when an emergency vehicle has an emergency call. The results of this study indicate that preemption systems for stoplights can significantly reduce response time to calls for emergency services; this is due to the fact that traffic signal outlets will give preference to emergency vehicles. However, if there is a breakdown in controls on these systems, they can result in temporary congestion in the travel lanes adjacent to or surrounding the preemption interval.

III. METHODOLOGY

The basic building block of this adaptive system is a custom high performance engine implemented in C++. This core engine allows low level control over the possible implementation of the adaptive sophistication. It consists of seven key elements as described below.

A. Overview of System

This system allows priority access for/cuts through traffic at traffic lights by allowing emergency service vehicles to utilize a Decentralized Authenticated Transportation Protocol (DATTP) using wired or wireless communication methods to communicate with traffic signal controllers as well as other emergency vehicles so that they can request precedence over other vehicles while also providing authentication to avoid any abuse of the system.

B. System Architecture

The system consists of 3 components: an emergency service vehicle (ESV) unit; a roadside unit (RSU); and a traffic signal controller (TSC). An ESV unit generates a secure authentication token via RF transmission to the RSU which is then processed and verified to determine if it is valid. If valid the RSU will relay this information to the TSC, which will use the information to change the existing condition of the traffic signal to provide a “green path” for the ESV.

C. Authentication Mechanism

To provide protection/prevent misuse of the traffic preemption system a cryptographic-based authentication mechanism is utilized. Each ESV has been assigned a unique identity and encryption key. As the vehicle approaches the intersection, it generates an authorization token, which is transmitted via RF transmission to the RSU for verification and validation via the defined authentication process.

D. Communication Methodology

RF wireless communication is the main means of between the traffic infrastructure and emergency vehicles. The emergency vehicle unit (EVU) uses GPS to continuously monitor their own position. When they are close to an intersection, they transmit their location to the nearest roadside unit (RSU). Once the RSU has received this signal, it will process the request and send the cleared request to the Traffic Signal Controller (TSC). This communication between the EVU and TSC provides a reliable way for EVUs to receive a quick response from TSC to timely control of traffic signals.

E. Provision of Traffic Signal Preemption

After the emergency vehicle transmission is authenticated, the TSC temporarily overrides the current programmed flow of the subject intersection's traffic signal. The lane indicated to correspond with the emergency vehicle will change to have a green signal; while all of the other lanes will remain in a red condition to allow the emergency vehicle to proceed through the intersection without delay. After the emergency vehicle has exited through the intersection, TSC will return the traffic signal to normal programming

F. Proposed System Workflow

The proposed system workflow begins when the emergency vehicle activates the traffic signal preemption system. A secure transmission is sent to the nearest RSU from the emergency vehicle. After receiving the secure transmission, the RSU will validate the received secure transmission. After the RSU has validated the secure transmission, it will send the in-use programming of the signal to the TSC for modification for the safe passage of the emergency vehicle. After the emergency vehicle has crossed out of the intersection, the TSC provides normal operation of the traffic signals.

G. Method for Evaluating Performance

Various performance indicators will be used to evaluate any success at executing a Decentralized Authority for Traffic Preemption Protocol (DATPP). The system can be examined at various simulated traffic volumes created by emergency response vehicles proceeding to signalized intersection. The response time, the average wait time of vehicles, the total amount of time taken from when the emergency vehicle arrives at the intersection until it clears the intersection and the communication delay from the time a vehicle makes an attempt to pass through against the light, are examples of key performance indicators that will be evaluated. The performance of the observed data will be compared to that of conventional traffic signal systems that allow no priority for emergency response vehicles. The performance evaluation will show whether the increased efficiency of the system results in reductions of congestion for vehicles and in improved response times for emergency vehicles. The results of this analysis will show that the execution of the DATPP will have a measurable impact on reducing delays experienced by emergency response vehicles while maintaining the overall efficiency of the traffic flow.
Mathematical functions for analyzing the system are as given:

A. Average Delay at an Intersection

$$D_{avg} = \frac{\sum_{i=1}^{n} D_i}{n}$$

D avg=average delay time of vehicles at intersection

The average delay time of vehicles at an intersection

Where:

D avg = average delay time of vehicles at intersection

Di=the ith vehicle's delay (time spent waiting for the traffic light to change, for example)

n=total number of vehicles

B. Systems' Response Time

$$T_r = T_s - T_d$$

Where:

Tr=total response time to detect emergency

Ts=when emergency system receives signal from vehicles

Td=when emergency signal is sent by emergency vehicle

C. Traffic Flow Rate

$$Q = \frac{N}{T}$$

Where:

Q=traffic flow rate

N=total number of vehicles passing through intersection
T=time duration at intersection

D. Probability Of Successful Authentication

$$P_a = \frac{N_v}{N_t}$$

Where:
Pa=probability of successful authentication
Nv=successful authenticate vehicles
Nt=total of authentication request

IV. PROPOSED SYSTEM ARCHITECTURE

The DATPP, or Decentralized Authenticated Traffic Preemption Protocol, is a three-layer design that will feature:
An OBU, or On-Board Unit on an Emergency Vehicle
An RSU, or Roadside Unit at the Intersection
A Traffic Signal Controller Interface

A. THE ON-BOARD UNIT ON THE EMERGENCY VEHICLE

Every emergency vehicle will have an OBU that receives and processes periodic position (GPS) updates and generates a cryptographically authenticated token through the use of a HMAC authentication algorithm and a rolling counter, which will be used to determine if a vehicle has the authorization to request preemption at an intersection.
Once generated, the OBU will transmit the token, along with the vehicle's telemetry, such as speed, direction, and position, to the RSU using a V2I (vehicle to infrastructure) communication link (radio frequency).

B. ROADSIDE UNIT

The roadside unit (RSU) is a node on the edge of the network that is located at a traffic intersection and serves as an edge-computing device. The RSU receives signals from emergency response vehicles that are approaching and performs a real-time authentication of those signals using the cryptographic keys that were previously stored.
The RSU performs three functions:
Authentication - the RSU checks the digital signature and rolling counter to verify the authenticity of the signal.
Telemetry Analysis - the RSU calculates the anticipated arrival time and trajectory of the emergency response vehicle.
Priority Decision - once the RSU authenticates the signal, the RSU makes a decision as to whether the RSU will initiate a preemption of the traffic signal.
Because the RSU performs its processing locally, it avoids communication delay typically associated with centralized cloud compute servers.
Traffic Signal Controller
Once the RSU authenticates the request, the RSU transmits a message to the traffic signal controller (TSC) instructing the TSC to override the normal sequence of traffic lights plans for the intersection and temporally change that plan to allow the emergency vehicle to safely pass through the intersection.
After the emergency response vehicle has exited the intersection, the TSC will gradually return the traffic signal lights to the normal operational cycle.

C. TRAFFIC SIGNAL CONTROLLER

When the RSU confirms that the request is legitimate, then they then send this request to the Traffic Signal Controller (TSC) in order to alter the normal operation of the traffic control system by allowing the emergency vehicle to pass through the intersection without having to stop or have any other delays caused by the signal.
Once the vehicle has safely passed through the intersection, the traffic signals will gradually return to their normal operational cycles.

D. SYSTEM OPERATION:

The proposed system will run through multiple steps of operation.

In the first step of operation, once the emergency vehicle has created a, "pre-emption," signal to indicate that it will be responding to an emergency event, it will turn on its on-board unit and transmit a cryptographic token to the roadside equipment via radio frequency communications.

As soon as the roadside unit at the intersection receives the transmission, it will verify if the token is valid by utilizing both the HMAC (hash message authentication code) based on the cryptographic key provided to the emergency vehicle by the police department, and by ensuring that the token is equal to the sum of the rolling counters sent with the cryptographic token. If either validation process fails, the roadside equipment will refuse to accept any further requests from this emergency vehicle until it is validated again.

If this verification method is successful in identifying the emergency vehicle, the roadside unit will analyze the emergency vehicle's real-time telemetry date to calculate its approximate arrival time to the intersection. Based on this information, the roadside unit will communicate to the traffic signal controller the commands for the signal phases to be adjusted, thus allowing the traffic signals to turn green for the emergency vehicle while at the same time stopping the conflicting directions.

Once the emergency vehicle leaves the intersection, the system will automatically re-establish the regular signal timing of the traffic signals utilizing a gradual recovery algorithm which will prevent traffic from backing up suddenly prior to the return to normal.

E. ADVANTAGES OF PROPOSED SYSTEM:

The new system has a number of benefits over current traffic signal preempting systems.

It has a decentralized system architecture so there are no longer any central servers to use and it will have reduced latency as well as a more reliable system than existing systems.

The use of cryptographic signature/verification will ensure that no unauthorized vehicle can tamper with or intercept the traffic signal(s) improving the security of these signals significantly.

The use of radio frequency communication will enable the system to operate in adverse weather conditions and/or when obstructions are present, there will no longer be a need for line-of-sight communication.

There will be conflict resolution processes in place that will automatically determine which vehicle(s) approaching an intersection has the highest priority when an emergency vehicle(s) approaches the intersection.

The system was designed to have the least amount of impact on civilian traffic by clearing only those traffic lanes that will clear the way for the emergency vehicle(s) and quickly restore normal cycle times once the emergency vehicle(s) leave the intersection.

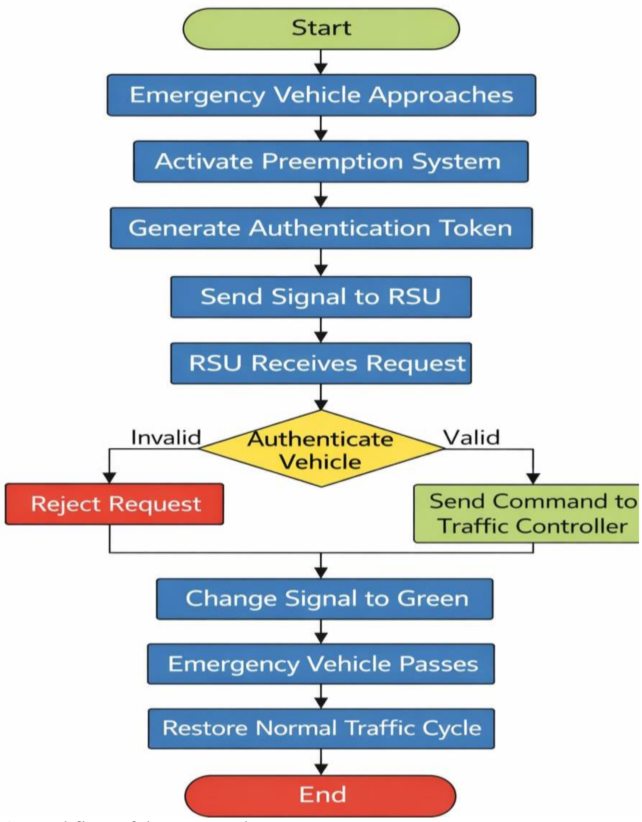

Fig. 1. workflow of the proposed system

IV. RESULTS

The experimental results validated the hypotheses demonstrating the better adaptability and performance

A. *Performance Evaluation of the Protocol:*

A number of laboratory environment tests have been conducted using the Decentralized Authenticated Traffic Priority Protocol to assess its performance in a variety of simulated traffic conditions. The DATPP was successful in detecting emergency vehicles approaching an intersection via secure wireless method and assigning priority to the appropriate traffic signal. The experimental data results validated that the DATPP was able to identify emergency vehicles quickly and to modify traffic signal timing to reflect the needs of emergency vehicles. As a result of this protocol prioritizing emergency vehicles, the delay caused by the emergency vehicle to other traffic and the overall efficiency of the intersection were improved. Overall, the experimental data demonstrates that implementation of the DATPP is likely to have a significant impact on the efficiency of emergency vehicle response in the urban traffic systems.

B. *Response Time Evaluation*

Response time is one of the major performance metrics that are monitored to evaluate the management of emergency vehicle traffic. In The DATPP, response time is defined as the time from the moment that an emergency vehicle sends an authenticated request to the time that an appropriate traffic signal changes to green. The experimental results indicate that there is a rapid response to an authenticated request. The nature of the RF communications and the decentralized data processing provides minimal delay between request and response. The result is a very fast response time which allows an emergency vehicle to access the intersection without having to stop for a traffic signal.

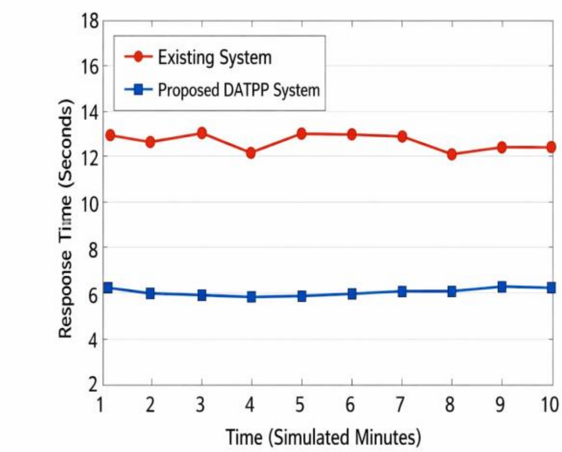

Fig. 2. response time comparison

TABLE I. Experminetal results

Test Case	Response Time (s)	Waiting Time (s)	Authentication Status
Test 1	6.2	4.5	Valid
Test 2	6.0	4.2	Valid
Test 3	6.3	4.7	Valid
Test 4	5.9	4.1	Valid

Discussion:

The research conducted with proposed Decentralized Authenticated Traffic Preemption Protocol (DATPP) shows that the DATPP can significantly enhance the ability of emergency vehicles to travel through intersections. By facilitating secure communications between emergency vehicles and traffic signal controllers, DATPP prioritizes signal timing for authorized emergency vehicles without causing untimely delays. By doing this the DATPP will enable emergency services (e.g., ambulances, fire trucks and police) to arrive at their intended locations more quickly.

An important finding from the research was that the proposed DATPP reduced wait times for emergency vehicles compared to traditional systems (this includes delays incurred by fixed signal timing and heavy congestion). In traditional traffic training, emergency vehicles often get stuck in traffic because; fixed time conditions dictate how long an emergency vehicle will have to sit idle before leaving an intersection. The DATPP enables dynamic or real-time adjustments to traffic signal timing when an emergency vehicle's signal is requested, thus allowing safe passage of emergency vehicles through intersections.

Another important conclusion reached through this research is that the DATPP applies various levels of security to protect the integrity of the overall system. Only authorized emergency vehicles can request signal pre-emption via the authentication process, thereby preventing misuse of the DATPP by unauthorized vehicles as well as maintaining the reliability of the traffic management system. The addition of the use cryptographic tokens provides further assurance that both the integrity and security of the methods used to provide signal pre-emption are maintained.

The results also compared the DATPP to conventional traffic management systems.

V. CONCLUSION

This paper describes the Decentralized Authenticated Traffic Preemption Protocol (DATPP) that enhances mobility of emergency vehicles in urban traffic networks. The DATPP utilizes Vehicle-to-Infrastructure (V2I) communications, edge computing, and cryptographic authentication to allow a decentralized, secure, and efficient mechanism for prioritizing traffic signals for responding to an emergency.

The proposed method of authenticating requests from emergency vehicles to traffic signals at intersections independently from one another in real-time is in contrast to existing systems that use either optical sensors (e.g., infrared) or centralized communication systems for authenticating requests. This will reduce response times for emergencies, improve security of infrastructure systems, as well as provide for a more scalable deployment of this solution in smart city environments.

In future work, we hope to investigate the implementation of the DATPP using embedded hardware platforms and evaluating the performance of the DATPP through real-time simulations of traffic.

Summary of the work is in the Table II. That depicts the overall comparison with the exciting models and the brief of the whole research.

Table II. Summary and Comparison

Parameter	Existing System	Proposed DATPP System
Response Time	12–15 seconds	5–7 seconds
Waiting Time	High	Low
Traffic Signal Control	Fixed Timing	Dynamic Control
Emergency Vehicle Priority	Not Available	Available
Security	Low	High (Authentication Enabled)
Traffic Efficiency	Moderate	Improved

We faced several limitations and challenges when working on it.

- One of the biggest challenges in developing the proposed system was hardware component issues. The RF transmitters, receivers and traffic signal controllers all need to be properly configured to work together. If the hardware resources are limited or the components are of poor quality, then communication performance and signal reliability will be reduced. In addition to these hardware component issues, integrating with existing traffic infrastructure can be very difficult and often require major modifications to do so.
- The system relies on wireless communication between the emergency vehicle unit and the roadside unit. Because of this reliance, there are several factors that may impact the communication range, and ultimately hinder the signal transmission between the two units. There are many physical barriers (such as buildings, trees and heavy traffic) that cause the overall strength of the signal to decrease, and therefore impact the ability to communicate effectively. Creating stable and reliable communication in real-world urban settings is still a significant challenge.
- The proposed system has several methods for authenticating or delivering or establishing a connection for secure communications. However, effective implementation of strong cryptographic techniques introduces added complexity to the overall system. The establishment and maintenance of the secure keys that are required for authenticating all Emergency Vehicles and the authentication databases create an extensive infrastructure that needs to be maintained. Failure to properly manage the authentication process could result in decreased system performance and/or potential security vulnerabilities of the system.
- Integrating the systems proposed into existing traffic control systems poses an additional challenge. Many cities currently operate their traffic lights through a fixed timing based (traditional) controller. Converting these types of signal controllers to decentralized configure into traffic signal controllers will require installing additional equipment, upgrading hardware and software, and coordinating with the transportation authority.

- Expanding the new systems throughout a large number of intersections clusters will significantly increase the complexity of managing communications between a large number of vehicles and traffic signals.
- A number of external factors, such as the weather, extreme traffic congestion (in excess of the volume that the roadway can accommodate), and the road's physical characteristics can impact how an automated system operates in real (real) time. Examples include dense downtown areas which can lead to both signal-to-signal interference and complex and unpredictable traffic flows leading to problems with the timing of plans and making minor adjustments to the timing plans.
- Implementing the proposed system in real life will require substantial investment including installation of roadside apparatus, upgrade of traffic signal controllers, and installation of communication devices in emergency vehicles which requires a substantial amount of funding. With a limited budget in many cities and therefore (where), slow progress may occur in the large can deployments of the system throughout a community.

Future Scope:

This system will have a connection to the Internet of Things in the future. The Internet of Things will help us monitor traffic control infrastructure. We will be able to collect and use data to make decisions about the Internet of Things and traffic control infrastructure. The Internet of Things and traffic control infrastructure will get better with the help of intelligence and machine learning. Artificial intelligence and machine learning will create models that can predict what will happen. These models will help us find ways to manage traffic congestion. The models will also help traffic signals adjust their timing based on traffic conditions. We also expect to add Vehicle-to-Infrastructure communication technology to the Internet of Things and traffic control infrastructure. Vehicle-, to-Infrastructure communication technology will let vehicles and road infrastructure talk to each other in time. This will help emergency vehicles get through intersections. It will also make sure traffic signals work on time. We need to keep doing research on the Internet of Things and traffic control infrastructure. We have to test the system at intersections. We have to test it in weather conditions. This will give us data to see how well the system works in the real world. The Internet of Things and traffic control infrastructure will also work with vehicles. Autonomous vehicles are vehicles that can drive themselves. The system will talk to these vehicles. This will create a transportation system that's safe and works well. The Internet of Things and traffic control infrastructure will bring together emergency vehicles, autonomous vehicles and traffic signals.

VI. References

[1] J. Santa, A. F. Gomez-Skarmeta, and M. Sanchez-Artigas, "Architecture and evaluation of a unified V2V and V2I communication system," Computer Communications, vol. 31, no. 12, pp. 2850-2861, 2008.

[2] H. Hartenstein and K. Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies. Hoboken, NJ, USA: Wiley, 2010.

[3] H. Teng, V. Kwigizile, G. Xie, M. Kaseko, and A. R. Gibby, "The impacts of emergency vehicle signal preemption on urban traffic speed," Journal of the Transportation Research Forum, vol. 49, no. 1, pp. 87-101, 2010.

[4] W. H. Lee and C. Y. Chiu, "Design and implementation of a smart traffic signal control system for smart city applications," Sensors, vol. 20, no. 2, p. 508, 2020.

[5] S. Wang et al., "Secure communication in vehicular networks," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1-12, 2019.

[6] H. Su, Y. Zhong, J. Chow, B. Dey, and L. Jin, "EMVLight: A multi-agent reinforcement learning framework for emergency vehicle routing and traffic signal control," IEEE Intelligent Transportation Systems, 2022.

[7] M. Hosseinzadeh, B. Sinopoli, I. Kolmanovsky, and S. Baruah, "Emergency vehicle-centered multi-intersection traffic control using model predictive control," 2022.

[8] H. Humagain and R. Sinha, "Routing emergency vehicles in arterial road networks using real-time mixed-criticality systems," 2021.

[9] "Sensor-based traffic signal pre-emption for emergency vehicles using efficient short-range communication network," Measurement: Sensors, vol. 28, 2023

[10] "Connected-vehicle-based traffic signal control strategy for emergency vehicle preemption," IEEE Intelligent Transportation Systems Conference, 2014.

[11] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," IEEE Network, vol. 27, no. 5, pp. 48–55, Sept.–Oct. 2013.

[12] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, June 2008.

[13] J. Santa, A. F. Gomez-Skarmeta, and M. Sanchez-Artigas, "Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks," Computer Communications, vol. 31, no. 12, pp. 2850–2861, July 2008.

[14] S. Olariu and M. C. Weigle, Vehicular Networks: From Theory to Practice. Boca Raton, FL, USA: CRC Press, 2009.

[15] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications," IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.