Kashf Journal of Multidisciplinary Research
Vol: 03 - Issue 03 (2026)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

RESCUE FACILITATION THROUGH AUTONOMOUS VEHICULAR AD HOC NETWORKS

***Saeed Ur Rehman*[1], **Dr Anum Ali*[2]**

[1, 2]*Department of Computer Science, Lahore Leads University, Pakistan*

[*]***Corresponding Author:*** (dranumali.cs@leads.edu.pk)

DOI: (*https://doi.org/10.71146/kjmr980*)

Article Info

Abstract

The rapid development of wireless communication networks has facilitated the emergence of Vehicular Ad Hoc Networks (VANETs), enabling critical applications in road safety, traffic efficiency, and intelligent transportation systems. Among these applications, the facilitation of emergency services, particularly ambulance routing and path clearing, stands out as a crucial area where rapid data transmission can directly save lives. However, achieving reliable and secure ambulance traversal through congested urban environments presents significant challenges, primarily due to the high mobility of network nodes and the constant threat of cyber-attacks. This paper proposes a comprehensive framework for ambulance rescue operations leveraging a network of autonomous vehicles connected via VANET. By systematically reviewing existing literature on routing protocols, network topology governance, and cybersecurity, this study develops a multi-layered approach that integrates secure broadcasting, dynamic topology adjustment, and cooperative vehicle dispersal. Furthermore, a hypothetical evaluation plan is presented to rigorously test the proposed framework using advanced simulation tools. Ultimately, this research highlights the necessity of secure, scalable, and dynamically adaptable VANET architectures to support the life-saving missions of emergency response vehicles in future smart cities.

Keywords:
rescue, vanet, emergency, adhoc network, ambulance.

Introduction

Recent years have witnessed rapid developments in wireless technologies, which have made Inter-Vehicular Communications (IVC) and Road-Vehicle Communications (RVC) highly feasible within the broader domain of Mobile Ad Hoc Networks (MANETs) (Samara 2012). This technological evolution has given birth to Vehicular Ad Hoc Networks (VANETs), a specialized class of MANETs characterized by rapidly changeable topologies and distinct mobility patterns (Moawad et al. 2013). The primary objective of VANETs is to improve the driving environment by enabling road safety, providing infotainment, and supporting efficient transportation management (Samara and Al-Raba'nah 2017). Given the alarming global statistics regarding traffic accidents and fatalities, deploying intelligent transportation systems that can seamlessly communicate emergency information has become an urgent societal priority (Samara 2012).

In the context of urban environments, one of the most critical challenges is ensuring the rapid and unimpeded traversal of emergency vehicles, particularly ambulances, through severe traffic congestion. The problem scope of this paper centers on utilizing an interconnected network of autonomous vehicles (AVs) to autonomously detect, negotiate, and clear paths for approaching ambulances. Within a conventional traffic system, human drivers often suffer from delayed reaction times and a lack of situational awareness regarding the exact trajectory of an approaching emergency vehicle. By integrating AVs into a localized VANET, vehicles can theoretically receive early warnings, coordinate their movements using advanced clustering strategies (Mukhtaruzzaman and Atiquzzaman 2020), and physically move out of the ambulance's designated lane before the emergency vehicle even arrives.

Despite the theoretical promise of VANETs in emergency response, existing approaches remain vastly insufficient for fully autonomous ambulance facilitation. First, traditional routing protocols inherited from MANETs are generally unsuitable for the high-speed, highly dynamic environment of VANETs, leading to frequent link breakages and delayed emergency message dissemination (Moawad et al. 2013). Second, existing vehicular communication systems suffer from severe security and trust vulnerabilities, as malicious actors can launch impersonation attacks to hijack emergency priority signals, a threat that is further exacerbated by the advent of quantum computing (Shakib et al. 2023). Furthermore, current network topology models often generate fixed degree distributions, lacking the autonomous adaptability required to prioritize low-latency emergency broadcasts in diverse traffic scenarios (Ren et al. 2026).

To address these critical shortcomings, this paper proposes a specialized operational framework tailored for ambulance rescue through autonomous VANETs. Specifically, the contributions of this paper are articulated as follows:

- This study introduces a multi-layered emergency broadcasting framework that dynamically adjusts the network's localized topology to ensure low-latency message propagation to surrounding autonomous vehicles.

- This paper presents a structured, hypothetical evaluation methodology that leverages advanced cloud-based simulation environments and realistic mobility models to validate the efficacy of emergency path-clearing algorithms.

Related Work

Routing Protocols and Mobility Models

The foundation of effective VANET communication lies in the design of robust routing protocols and realistic mobility models. Traditional ad hoc routing protocols are often inadequate for VANETs due to the special mobility patterns of vehicles and the rapidly changing network topology (Moawad et al. 2013). To address this, researchers have proposed modified protocols, such as SSD-AOMDV, which incorporate mobility parameters like stop times, speed, and direction to better select the next communication hop during route discovery (Moawad et al. 2013). Furthermore, the accuracy of testing these routing protocols heavily relies on the applied mobility models, which define the movement patterns of the vehicles in simulations (Danquah and Altilar 2014). While standard urban and highway models exist, hybrid approaches like the HYBRIST mobility model have been proposed to bridge the vast differences in mobility patterns, ensuring more accurate and realistic simulation results (Danquah and Altilar 2014). Although these routing and mobility advancements significantly improve general packet delivery, they do not inherently provide the specialized preemptive physical path-clearing mechanisms required for emergency ambulance operations.

Topology Governance and Network Science

Effective management of network structure is vital for ensuring that emergency messages propagate rapidly without causing massive network congestion. Researchers have increasingly applied network science principles to study VANETs, analyzing metrics such as node degree distribution, clustering coefficients, and average shortest path lengths to optimize broadcast mechanisms (Monteiro et al. 2013). By understanding whether a vehicular network exhibits small-world or scale-free properties, protocols can be locally adjusted to significantly reduce broadcast storms without degrading overall performance (Monteiro et al. 2013). Additionally, the governance of localized VANETs requires a dynamic trade-off between network robustness against attacks and the need for low-latency information transmission (Ren et al. 2026). Recent models propose schedulable degree distributions using hybrid connection mechanisms, allowing the network to shift autonomously between uniform and power-law distributions depending on traffic scenarios (Ren et al. 2026). Furthermore, clustering algorithms that group vehicles based on shared features, often utilizing machine learning or fuzzy logic, have been developed to maintain hierarchical stability among highly mobile nodes (Mukhtaruzzaman and Atiquzzaman 2020). Compared to this prior work, our proposed approach synthesizes these dynamic topology adjustments specifically to forge temporary, high-priority communication tunnels ahead of an active ambulance.

Security, Trust, and Spectrum Coexistence

The practical deployment of emergency VANET systems is heavily contingent upon resolving inherent security challenges and spectrum limitations. Security is widely considered a critical point in the development of robust VANET systems, as vulnerabilities can directly endanger human lives (Samara and Al-Raba'nah 2017). Beyond traditional attacks, modern blockchain-based VANET architectures, which are generally considered secure, face looming threats from quantum computing, where algorithms like Shor's can break RSA encrypted digital signatures and execute impersonation attacks (Shakib et al. 2023). In addition to security, spectrum scarcity poses a severe bottleneck for massive vehicular data transmission. To support cellular vehicle-to-everything (V2X) users, the utilization of unlicensed spectrum has been explored to facilitate harmonious coexistence with standard VANET users through energy sensing and dynamic vehicle-resource matching algorithms (Wang et al. 2017). The approach proposed in this paper integrates these security and spectrum considerations by mandating cryptographically secured emergency beacons that utilize optimized unlicensed spectrum channels to bypass saturated standard communication bands.

Method/Approach

Framework Overview

To effectively facilitate ambulance rescue operations, we propose the Autonomous Cooperative Path-Clearing (ACPC) framework. This framework operates as a multi-layered, structured pipeline designed to securely alert surrounding autonomous vehicles and coordinate their physical dispersal to create a free lane. The ACPC system integrates communication, topology management, and physical actuation into a cohesive sequence. By decentralizing the decision-making process to localized clusters of AVs, the system minimizes latency and avoids the single points of failure typically associated with centralized traffic management centers.

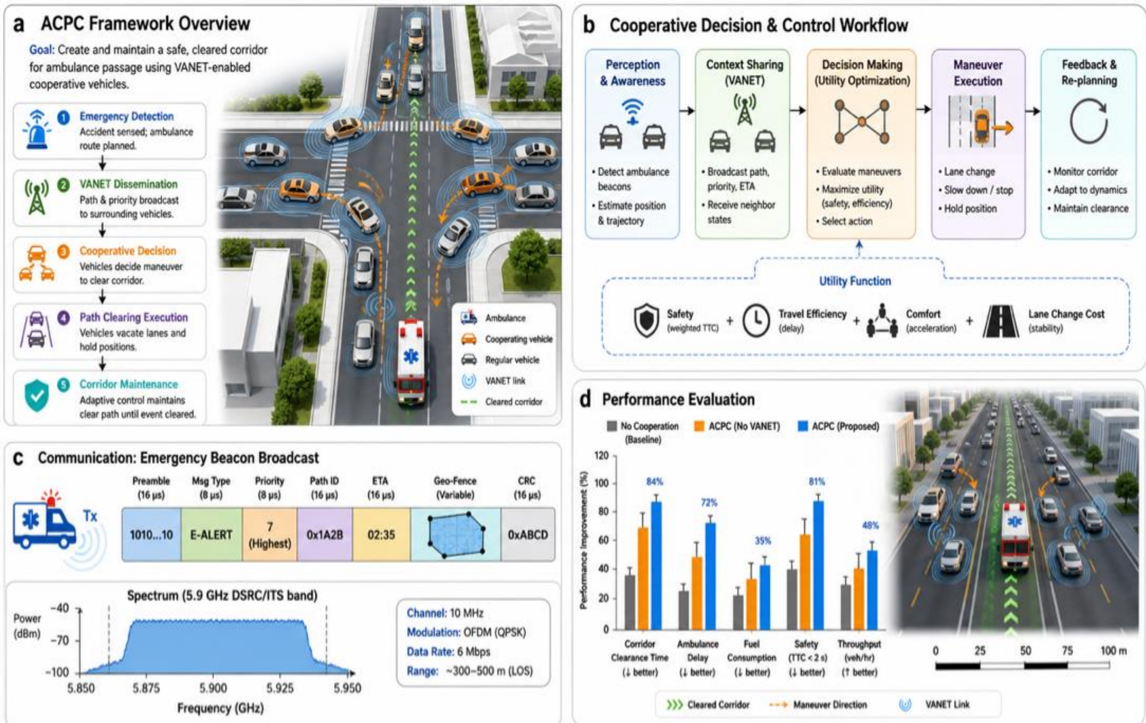

Fig1: Autonomous Cooperative Path-Clearing (ACPC) framework

Module 1: Secure Emergency Beaconing and Authentication

The first step in the pipeline is the initiation of an encrypted Emergency Rescue Beacon (ERB) by the ambulance. Because standard digital signatures are increasingly vulnerable to advanced threats, including potential quantum cyber-attacks (Shakib et al. 2023), the ERB utilizes a quantum-resistant cryptographic hashing mechanism to ensure its authenticity. When the ambulance activates its emergency sequence, it temporarily acts as a paramount Cluster Head, broadcasting the ERB to all surrounding vehicles and Road Side Units (RSUs) via both dedicated short-range communications (DSRC) and available unlicensed cellular V2X spectrum (Wang et al. 2017). This dual-channel approach ensures that the critical message bypasses localized congestion and reaches vehicles at multiple distances. Upon receiving the ERB, autonomous vehicles immediately verify the signature to prevent malicious impersonation attacks that could otherwise cause unwarranted traffic disruptions.

Module 2: Topology Adjustment and Path Clearing

Once the surrounding network authenticates the ERB, the local VANET topology undergoes a rapid, autonomous reconfiguration. Utilizing an adjustable degree distribution model, the network dynamically shifts its underlying topology to prioritize the ambulance as a hub node, thereby dramatically shortening the transmission path lengths for continuous coordinate updates (Ren et al. 2026). The autonomous vehicles then execute a cooperative maneuvering algorithm based on the ambulance's broadcasted speed, direction, and predicted trajectory. Vehicles occupying the target lane autonomously negotiate with adjacent vehicles to safely merge into neighboring lanes or pull over to the road shoulder. This physical dispersal is synchronized using localized multi-hop clustering strategies (Mukhtaruzzaman and Atiquzzaman 2020), ensuring that vehicles do not accidentally collide while attempting to yield to the emergency vehicle.

Evaluation Plan

To rigorously validate the ACPC framework, we propose a hypothetical evaluation plan leveraging state-of-the-art simulation environments. Due to the high computational requirements of calculating hierarchies among mobile vehicles, a cloud-based VANET simulator, such as the CVANETSIM architecture, provides an ideal platform for processing large-scale, real-time vehicular data (Mukhtaruzzaman and Atiquzzaman 2021). The simulation will be integrated utilizing a combined platform of OMNeT++, Vehicles-in-Network Simulation (VEINS), and the Simulation of Urban Mobility (SUMO) traffic simulator, mimicking the methodology used in advanced cybersecurity evaluations (Shakib et al. 2023). We will utilize the HYBRIST mobility model to inject near-reality movement patterns, transitioning seamlessly between urban and highway scenarios to test the framework's adaptability (Danquah and Altilar 2014). The core benchmarking metrics will include the average delay in ambulance traversal, the reduction of broadcast storm overhead (Monteiro et al. 2013), and the success rate of cryptographic beacon verification under simulated high-congestion scenarios.

Discussion

Practical Implications and Deployment Considerations

The deployment of the proposed ACPC framework carries profound practical implications for the future of intelligent transportation systems and smart city infrastructure. By effectively integrating ambulances into an autonomous VANET, cities can drastically reduce the response times of emergency medical services, directly correlating to higher patient survival rates. From a deployment perspective, this system necessitates the harmonious coexistence of diverse communication standards, specifically the integration of standard IEEE 802.11p DSRC with emerging 5G Cellular V2X technologies over unlicensed spectrums (Wang et al. 2017). Policymakers and automotive manufacturers must collaborate to establish universal standards for emergency beaconing, ensuring that vehicles from different manufacturers can flawlessly interpret and act upon the same path-clearing requests.

Limitations and Failure Modes

Despite its robust design, the proposed framework exhibits several limitations and potential failure modes that must be carefully managed. First, the system remains susceptible to sophisticated cyber-threats; even with advanced encryption, the rapid evolution of quantum computing threatens the fundamental trust chains of blockchain-based vehicular networks, potentially allowing adversaries to spoof emergency vehicles (Shakib et al. 2023). Second, in extreme high-density urban environments, the sheer volume of simultaneous communication may trigger broadcast storms, leading to packet collisions and significant packet loss despite network science optimizations (Monteiro et al. 2013). Third, physical spatial limitations present a severe failure mode; in narrow, single-lane roads bordered by physical barriers, autonomous vehicles may logically receive the command to yield but physically lack the geometric space to clear a path, rendering the communication framework temporarily moot.

Ethical Considerations and Risks

Implementing an autonomous prioritization network introduces complex ethical considerations that society must navigate. The most prominent ethical risk involves the potential misuse of emergency priority privileges. If a malicious actor successfully exploits the network to impersonate an ambulance, they could forcefully manipulate the physical movements of surrounding autonomous vehicles, causing massive traffic blockages or even forcing vehicles into dangerous situations (Shakib et al. 2023). Furthermore, there is a distinct privacy risk associated with the continuous broadcasting of vehicular locations and patient-related emergency routes (Samara 2012). Striking a balance between the transparent data sharing necessary for network efficiency and the fundamental privacy rights of individual citizens remains a critical ethical hurdle for widespread VANET adoption.

Future Work

Future research must focus on fortifying the foundational vulnerabilities identified in this framework to ensure absolute reliability in life-or-death scenarios. One crucial area of future work is the development and integration of quantum-secured blockchain architectures tailored specifically for the extreme low-latency requirements of

VANETs, thereby neutralizing the threat of quantum cyber-attacks (Shakib et al. 2023). Additionally, researchers should focus on enhancing the physical mobility models used in simulations by further refining hybrid approaches, such as the HYBRIST model, to include complex edge cases like construction zones and adverse weather conditions (Danquah and Altilar 2014). By continuously iterating on both the digital security and physical simulation fronts, the academic community can bring autonomous emergency facilitation closer to real-world realization.

Conclusion

The integration of Vehicular Ad Hoc Networks (VANETs) into urban traffic management holds transformative potential for emergency response operations. This paper has comprehensively explored the facilitation of ambulance rescue missions through a localized network of autonomous vehicles. By analyzing the critical intersections of routing protocols, network topology governance, and cybersecurity, we proposed a multi-layered framework designed to securely broadcast emergency beacons and dynamically reconfigure the network to clear physical paths for ambulances.

While significant challenges remain—such as vulnerabilities to quantum cyber-attacks, spectrum coexistence limitations, and the physical constraints of urban infrastructure—the structured methodology provided herein offers a viable pathway forward. The hypothetical evaluation plan highlights the necessity of utilizing advanced, combined simulation platforms to rigorously test these life-saving algorithms in realistic hybrid mobility scenarios. Ultimately, as autonomous vehicles become increasingly prevalent, equipping them with secure, cooperative emergency response capabilities will be an indispensable step in constructing the intelligent, resilient cities of the future.

References

Samara, Ghassan. "Security Analysis of Vehicular Ad Hoc Networks (VANET)." 2012. https://doi.org/10.1109/NETAPPS.2010.17

Moawad, Hafez, et al. "Stop_times based Routing Protocol for VANET." International Journal of Computer Applications 81(18):4-9, November 2013. Published by Foundation of Computer Science, New York, USA, 2013. https://doi.org/10.5120/14221-2029

Samara, Ghassan, and Yousef Al-Raba'nah. "Security Issues in Vehicular Ad Hoc Networks (VANET): a survey." International Journal of Sciences & Applied Research, 2015, 2017. https://arxiv.org/pdf/1712.04263v1

Mukhtaruzzaman, Mohammad, and Mohammed Atiquzzaman. "Clustering in VANET: Algorithms and Challenges." Computers & Electrical Engineering, Volume 88, December 2020, 106851, 2020. https://doi.org/10.1016/j.compeleceng.2020.106851

Shakib, Kazi Hassan, et al. "Quantum Cyber-Attack on Blockchain-based VANET." 2023. https://arxiv.org/pdf/2304.04411v2

Ren, Ruixing, et al. "Towards Governance of Localized VANET: An Adjustable Degree Distribution Model." 2026. https://arxiv.org/pdf/2601.21176v1

Danquah, Wiseborn Manfe, and Turgay D Altilar. "HYBRIST Mobility Model- A Novel Hybrid Mobility Model for VANET Simulations." IJCA 86(14):15-21, January 2014, 2014. https://doi.org/10.5120/15053-3408

Monteiro, Romeu, et al. "Improving VANET Protocols via Network Science." R. Monteiro, S. Sargento, W. Viriyasitavat, and O. K. Tonguz, "Improving VANET Protocols via Network Science", in Proceedings of the 2012 IEEE Vehicular Networking Conference (VNC), Korea, November 2012, 2013. https://doi.org/10.1109/VNC.2012.6407428

Wang, Pengfei, et al. "Cellular V2X in Unlicensed Spectrum: Harmonious Coexistence with VANET in 5G systems." 2017. https://arxiv.org/pdf/1712.04639v2

Mukhtaruzzaman, Mohammad, and Mohammed Atiquzzaman. "Cloud based VANET Simulator (CVANETSIM)." 2021. https://arxiv.org/pdf/2101.11147v1